S04P0878W000

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2002－217894
（Ｐ２００２－２１７８９４Ａ）
(43)公開日　平成14年８月２日(2002.8.2)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
H04L 9/08		G06F 13/00	520	B 5C052
G06F 13/00	520	17/60	302	E 5C053
17/60	302		332	5C064
	332		ZEC	5J104
	ZEC	H04N 5/76		Z

審査請求　未請求　請求項の数17　ＯＬ　（全43頁）　最終頁に続く

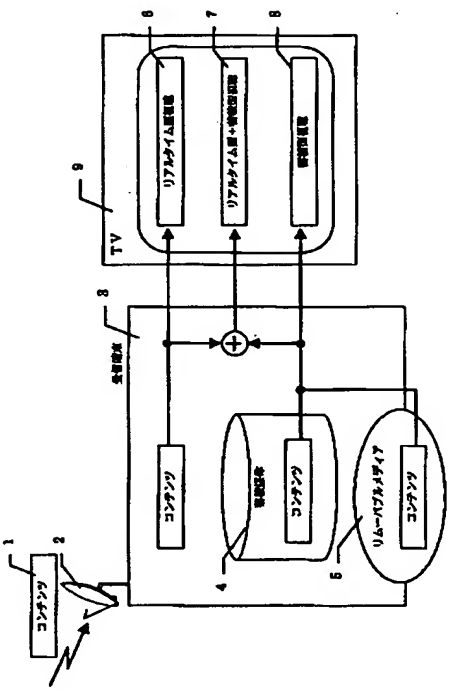
(21)出願番号　特願2001－295722(Ｐ2001－295722)
(22)出願日　平成13年９月27日(2001.9.27)
(31)優先権主張番号　特願2000－300566(P2000－300566)
(32)優先日　平成12年９月28日(2000.9.28)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　原田　宏美
東京都千代田区神田駿河台四丁目６番地
株式会社日立製作所放送・通信システム推進事業部内
(72)発明者　小西　薫
東京都千代田区神田駿河台四丁目６番地
株式会社日立製作所放送・通信システム推進事業部内
(74)代理人　100107010
弁理士　橋爪　健

最終頁に続く

(54)【発明の名称】データ配信サービス方法

(57)【要約】
【課題】　コンテンツに関する詳細な情報を用いてのコンテンツ制御サービスを行う。
【解決手段】　放送サイドで視聴者へのコンテンツ提示方法、利用条件、暗号化状態でのコンテンツ蓄積、端末に対する限定受信、個人に対する限定受信等を定義し、定義した内容をコンテンツと共に受信側に配信し、これらの定義に基づき視聴者の視聴制御、蓄積制御、コピー制御、暗号/復号制御等を行うことで著作権等のコンテンツの権利保護が可能なサービスを提供する。そのために、総合データ配信システムは、コンテンツ毎にコンテンツ関連情報であるメタデータを添付する。このメタデータには、コンテンツの名称、内容、コンテンツ内の構成等の一般的な情報や、蓄積再生処理に関する制御情報、課金処理に関する制御情報、コンテンツの復号鍵等のコンテンツ暗号方式に関する情報等の著作権保護に関する情報が記述される。



1

【特許請求の範囲】

【請求項１】衛星、地上回線等の通信回線もしくはリムーバブルメディア等のメディア媒体を用いてコンテンツの配信を行うデータ配信サービス方法において、

送信側装置は、

コンテンツの生成後にコンテンツの暗号化を行い、

暗号化されたコンテンツをブロック分けし、

配信ストリームのペイロード部分にブロック分けした暗号化コンテンツの各エレメントを格納して、配信データ形式に組み立て、コンテンツを配信し、

コンテンツの提示方法、利用条件、コンテンツの暗号鍵を含むコンテンツの関連情報を格納したメタデータを生成して配信し、

受信端末は、

コンテンツを組み立てる場合にペイロード部分を復号せずに組み立て、暗号化されたままの状態でのコンテンツ及びメタデータを蓄積し、

受信側でコンテンツの利用に関する判断をすることによりコンテンツに対する課金制御、権利保護を行うようにしたデータ配信サービス方法。

【請求項２】請求項１のデータ配信サービス方法において、

コンテンツの暗号化はコンテンツを構成する各エレメントのデータ全体に暗号化を行い、

メタデータについては予め定められた必要部分にのみ暗号化を行うことを特徴とするデータ配信サービス方法。

【請求項３】衛星、地上回線等の通信回線もしくはリムーバブルメディア等のメディア媒体を用いてコンテンツの配信を行うデータ配信サービス方法において、

受信端末は、ユーザーが有料事業者に対し契約した端末ID、個人ID、契約したいチャンネル又は番組又はコンテンツを含む契約要求を送出側装置に通知するステップと、

送出側装置は、通知された契約要求より事前契約用メタデータを生成し、端末ID、個人IDを非暗号化とし、有料事業者ID、事業者毎に固有の事業者鍵Kw、契約コードを含む契約情報を受信端末毎に固有の端末鍵Kmcで暗号化を行い、受信端末に配信するステップと、

受信端末は、事前契約用メタデータの非暗号化部分に格納されている端末ID、個人IDにより、端末を使用するユーザー宛の情報か否かを判断し、使用ユーザー宛と判断された場合は、受信端末内に予め格納されている端末鍵Kmcにより事前契約用メタデータを復号し、事業者鍵Kwを含む契約情報を入手するステップと、

受信端末は、入手した契約情報に基づき、契約事業者の放送するコンテンツの要求を行うステップと、

送出側装置は、暗号化コンテンツの配信と同期させ、有料事業者IDを非暗号化として含み、コンテンツを視聴する際に必要となるコンテンツの暗号鍵Kkを含む必要部分が事業者鍵Kwで暗号化された鍵配信用メタデータと、コンテンツ配信装置位置を含むコンテンツに対する利用制限情報を含む必要部分をコンテンツ鍵Kkで暗号化された蓄積/再生用メタデータとを配信するステップと、

受信端末は、暗号化コンテンツと同期させて配信される鍵配信用メタデータを受信し、非暗号化部分に格納されている有料事業者IDにより契約事業者による放送かを判断し、契約する事業者の放送するコンテンツに対する鍵配信用メタデータであると判断した場合、事前契約用メタデータにより配信された事業者鍵Kwにより暗号化部分を復号し、復号された対象契約コードと事前契約用メタデータにより配信された契約コードとによりユーザーの契約形態内で利用可能なコンテンツかを判断し、利用可能であればコンテンツ鍵Kkを受信端末に格納し、同時に受信した蓄積/再生用メタデータの暗号化部分をコンテンツ鍵Kkにより復号し、コンテンツに対する利用制限情報を確認し、ユーザーの利用が可能であれば、蓄積/再生用メタデータに格納されている暗号化コンテンツの配信場所の情報により暗号化コンテンツを受信するステップとを含むデータ配信サービス方法。

【請求項４】請求項１又は３に記載のデータ配信サービス方法において、

ユーザーに対して様々なコンテンツ単位、チャンネル単位、番組単位又はパソコンにおけるファイル単位などのエレメント単位のサービスを提供するために、送出側装置は、コンテンツの物理量を示す単位を指定し、指定した物理量をメタデータに含ませて配信することにより、受信端末が指定されたコンテンツ単位でサービスを提供可能とすることを特徴としたデータ配信サービス方法。

【請求項５】請求項１又は３に記載のデータ配信サービス方法において、

メタデータは、コンテンツのタイトル又は内容、送出側で定義した視聴者へのコンテンツ提示方法、利用条件を含む情報を含み、

送出側装置は、メタデータ自体もデータの改ざん防止、秘匿性保持のため必要部分を暗号化したのち配信し、

受信端末は、暗号化されたままの状態でメタデータを蓄積し、利用時に暗号鍵により受信端末を制御して権利保護を行うことを特徴とするデータ配信サービス方法。

【請求項６】請求項１又は３のデータ配信サービス方法において、

事前契約用メタデータは、有料放送事業者の事業者鍵Kw、契約形態に間する契約コード内容を含み、端末購入時、契約更新時又は事業者鍵Kwの更新時に配信されるメタデータであって、

EPG用メタデータは、配信予定コンテンツの確認又は予約を行うためのメタデータであり、

蓄積／再生用メタデータは、コンテンツの受信、蓄積、再生に必要な情報を含むメタデータであり、

鍵配信用メタデータは、コンテンツの暗号鍵に関する情報を配信するメタデータであり、

メタデータリストは、配信ストリーム中の各メタデータの配信位置を取得するためのメタデータであり、
システム鍵更新用メタデータは、全受信端末共通のシステム鍵Ksyを更新するためのメタデータであり、
送信側装置は、受信端末側での使用目的、送出側での配信タイミング、記述内容によりメタデータを、事前契約用メタデータ、EPG用メタデータ、蓄積/再生用メタデータ、鍵配信用メタデータ、システム鍵更新用メタデータ、メタデータリストに区分けして、配信することを特徴とするデータ配信サービス方法。

【請求項７】請求項６に記載のデータ配信サービス方法において、
ユーザーに対して個別に配信される事前契約用メタデータは、ユーザー個々の契約情報が格納され、全ユーザーに対して共通的に配信される各コンテンツに対する鍵配信用メタデータ、蓄積/再生用メタデータは、必要となる契約情報、利用条件等が格納され、事前契約用メタデータにより配信されたユーザー個々の契約情報と他のメタデータに含まれる契約情報とを照合してユーザーのコンテンツ利用を判断することで、ユーザー個々に対しコンテンツ単位の限定受信を行うようにしたことを特徴とするシステム。

【請求項８】請求項６に記載のデータ配信サービス方法において、
事前契約用メタデータは、ユーザー毎の契約情報や事業者毎の事業者鍵Kwを含む権利保護が必要な情報が格納され、送出側装置は、この情報を各ユーザーの所有する端末毎の端末鍵Kmc又は個人鍵Kmにより暗号化することにより情報の秘匿を守り情報を配信することを特徴とするデータ配信サービス方法。

【請求項９】請求項６に記載のデータ配信サービス方法において、
EPG用メタデータは、配信予定コンテンツの確認又は予約を行うもので、利用制限情報を含む権利保護が必要な情報が格納され、
送出側装置は、この情報を全受信端末で共通な鍵Ksyにより暗号化することによりユーザーの区別無く全ユーザーに対してメタデータ内の必要な情報の秘匿性を保持したまま配信することを特徴とするデータ配信サービス方法。

【請求項１０】請求項６に記載のデータ配信サービス方法において、
コンテンツに対する暗号鍵を含む情報を格納した鍵配信用メタデータ、コンテンツのコピーコントロール情報を含む情報を格納した蓄積再生用メタデータについて、送出側装置は、鍵配信用メタデータを事業者鍵Kw、蓄積再生用メタデータをコンテンツ毎のコンテンツ鍵Kkにより暗号化し配信することで、事業者と契約を行い事前契約用メタデータにより事業者鍵を受け取ったユーザーのみコンテンツ鍵Kkを取得可能とすることでコンテンツの権利保護を実現することを特徴とするデータ配信サービス方法。

【請求項１１】請求項６に記載のデータ配信サービス方法において、
鍵配信用メタデータは、コンテンツの暗号鍵に関する情報を配信するものであり、
送信側装置は、コンテンツが有料放送の場合は、その情報を事業者毎に固有の事業者鍵Kwにより暗号化し、契約者以外のユーザーも視聴可能な無料コンテンツに対するメタデータの場合は、全受信端末に共通なシステム鍵Ksyにより暗号化すること。

【請求項１２】請求項６に記載のデータ配信サービス方法において、
システム鍵更新用メタデータは、システム内の全受信端末で共通なシステム鍵を含むシステム全体で共通的な情報を更新するための情報が格納されたメタデータであり、
送信側装置は、新しいシステム鍵Ksy3を含む保護が必要な部分を予め全受信端末内で共通に用意された予備用のシステム鍵Ksy2を用いて暗号化することでユーザーの区別なくメタデータ内の必要な部分の秘匿性を保持したまま配信可能とすることを特徴とするデータ配信サービス方法。

【請求項１３】請求項６に記載のデータ配信サービス方法において、
メタデータリストは、配信中の各メタデータリストの伝送路上の配信位置を格納し、受信端末は、メタデータリストを用いてメタデータの取得を行うことを特徴とするデータ配信サービス方法。

【請求項１４】請求項６に記載のデータ配信サービス方法において、
メタデータリストにEPG用メタデータ、蓄積再生用メタデータ等の更新を識別するための情報を格納することにより更新されたメタデータのみ受信を行うことを可能とすることを特徴とするに記載のデータ配信サービス方法。

【請求項１５】請求項１又は３のデータ配信サービス方法において、
暗号化されたメタデータを、暗号化を行わないメタデータに再度埋め込み配信する場合と、別ファイルとして配信する場合とのいずれかにより配信すること。

【請求項１６】請求項１又は３のデータ配信サービス方法において、
送出側装置は、受信端末を購入したユーザーが端末ID、個人ID、契約したい事業者、コンテンツを利用するためのポイント数を含む情報を元に顧客情報を生成管理し、許諾するポイント数の情報を事前契約用メタデータに格納し、契約ユーザーの受信端末に配信し、
送出側装置は、コンテンツを配信する際に同期させ、配信させる蓄積/再生用メタデータにコンテンツを利用す

る際に必要となるポイント数の情報を格納して配信し、受信端末は、コンテンツを利用する際に、事前契約用メタデータにより配信されたポイント数より蓄積/再生用メタデータに格納されている必要ポイント数を減算し、コンテンツの再生を行うことで、事前契約用メタデータで配信されたポイント数の範囲でのコンテンツを視聴することを特徴とするデータ配信サービス方法。

【請求項１７】請求項１又は３データ配信サービス方法において、

送出側装置は、受信端末を購入したユーザーが端末ID、個人ID、契約したい事業者、コンテンツを利用するためのポイント数を含む情報を元に顧客情報を生成管理し、オンラインペイパービュー許諾として、課金情報送信時の送信先の情報を事前契約用メタデータに格納し、契約ユーザーの受信端末に配信し、

送出側装置は、コンテンツを配信する際に同期させ、配信させる蓄積/再生用メタデータにコンテンツを利用する際の課金情報を生成する元となる情報を格納し配信する受信端末は、コンテンツを利用する際に、蓄積/再生用メタデータに格納された課金情報を生成するための元となる情報に対し利用ユーザーのIDを含む情報を加え、事前契約用メタデータにより指定された送信先に対し地上回線を利用して送信することを特徴とするデータ配信サービス方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、コンテンツ提供側においてコンテンツを提供し、利用側においてコンテンツを受け取り、利用するためのデータ配信サービス方法に係り、特に、コンテンツを保護する仕組みを備え且つコンテンツにコンテンツ関連情報であるメタデータを付加して配信する仕組みを備えたデータ配信サービス方法に関する。

【０００２】

【従来の技術】従来、衛星波や地上波を用いた放送または通信は、リアルタイム放送が一般的であり、一部、蓄積型の通信が存在していた。蓄積型の放送や通信は、配信された番組や情報をユーザー自身の蓄積動作によって、大容量の蓄積媒体に蓄積することが可能である。よって、ユーザーが望む時にいつでも、番組を視聴することができる。

【０００３】リアルタイム放送のコンテンツの保護方法として、コンテンツに暗号をかける方式が一般的である。暗号をかけることにより、不正な視聴や改ざんなどが困難となる。コンテンツ暗号方式として、BSデジタル放送の限定受信方式であるCAS(Conditional Access System)がある。CASはコンテンツを第１の暗号方式で暗号化し、その暗号化コンテンツを復号するための第１の復号鍵を第２の暗号方式で暗号化する。そして、暗号化コンテンツと第１の鍵をユーザーに対して配信する。その

コンテンツを受信可能なユーザーは、予め第２の暗号方式の復号鍵である第２の復号鍵を保持している。よって、第２の復号鍵を保持しているユーザーのみ第１の復号鍵を受信することができ、第１の復号鍵を受信できたユーザーのみがコンテンツを受信することが可能である。このように、CASを用いることで、限定されたユーザーのみコンテンツを入手し視聴することが可能となり、視聴可能なユーザーをコントロールすることが可能である。また、BSデジタル放送では、コンテンツに関する情報としてSI（サービス情報）が定義されている。

【０００４】

【発明が解決しようとする課題】上述のような従来技術のCASは、リアルタイム放送で用いられている限定受信方式である。この方式はコンテンツの受信と同時にコンテンツの復号処理を行う。その際、ユーザーに対する受信コントロールは可能であるが、コンテンツを復号してしまうため再生コントロールができない。また、蓄積時にコンテンツが平文状態となってしまうのでコンテンツの保護ができない。

【０００５】また、現状の衛星デジタル放送の規格においては、コンテンツに関する情報を定義するための手段として、SIのみしか存在しない。このSIはコンテンツの関連情報ではあるがEPG（電子番組ガイド）用の情報なので、詳細に記述されているわけではない。様々なコンテンツに関する詳細な情報を定義する手段は放送規格においてはないため、コンテンツ毎の制御に基づいた木目細かいサービスを行うことができない。これにより、コンテンツに関する詳細な情報を用いてのコンテンツ制御サービスは行うことができない。また、既存型の放送はコンテンツをリアルタイムで視聴することを念頭においたサービスであるため、コンテンツの蓄積制御、コピー制御を行うための情報が乏しく蓄積型放送に使用するには不充分である。

【０００６】本発明は、以上の点に鑑み、蓄積型放送かつ、コンテンツの保護が可能となる制御情報を付加するデータ配信サービス方法を提供することを目的とする。

【０００７】

【課題を解決するための手段】本発明の総合データ配信システムは、暗号化した状態のコンテンツを受信し、その後蓄積媒体に蓄積し、コンテンツの再生時に初めて復号する暗号方式を提供する。また、コンテンツ毎にコンテンツ関連情報であるメタデータを添付する。このメタデータには、例えば、コンテンツの名称、内容、コンテンツ内の構成等の一般的な情報や、蓄積再生処理に関する制御情報、課金処理に関する制御情報、コンテンツの復号鍵等のコンテンツ暗号方式に関する情報等の著作権保護に関する情報が記述される。これらの情報に基づき視聴者の視聴制御、蓄積制御、コピー制御、暗号/復号制御等を行う。これよりコンテンツの権利保護、ユーザーの権利保護等が可能となる。

【０００８】本発明の第１の解決手段によると、衛星、地上回線等の通信回線もしくはリムーバブルメディア等のメディア媒体を用いてコンテンツの配信を行うデータ配信サービス方法において、送信側装置は、コンテンツの生成後にコンテンツの暗号化を行い、暗号化されたコンテンツをブロック分けし、配信ストリームのペイロード部分にブロック分けした暗号化コンテンツの各エレメントを格納して、配信データ形式に組み立て、コンテンツを配信し、コンテンツの提示方法、利用条件、コンテンツの暗号鍵を含むコンテンツの関連情報を格納したメタデータを生成して配信し、受信端末は、コンテンツを組み立てる場合にペイロード部分を復号せずに組み立て、暗号化されたままの状態でのコンテンツ及びメタデータを蓄積し、受信側でコンテンツの利用に関する判断をすることによりコンテンツに対する課金制御、権利保護を行うようにしたデータ配信サービス方法が提供される。

【０００９】本発明の第２の解決手段によると、衛星、地上回線等の通信回線もしくはリムーバブルメディア等のメディア媒体を用いてコンテンツの配信を行うデータ配信サービス方法において、受信端末は、ユーザーが有料事業者に対し契約した端末ID、個人ID、契約したいチャンネル又は番組又はコンテンツを含む契約要求を送出側装置に通知するステップと、送出側装置は、通知された契約要求より事前契約用メタデータを生成し、端末ID、個人IDを非暗号化とし、有料事業者ID、事業者毎に固有の事業者鍵Kw、契約コードを含む契約情報を受信端末毎に固有の端末鍵Kmcで暗号化を行い、受信端末に配信するステップと、受信端末は、事前契約用メタデータの非暗号化部分に格納されている端末ID、個人IDにより、端末を使用するユーザー宛の情報か否かを判断し、使用ユーザー宛と判断された場合は、受信端末内に予め格納されている端末鍵Kmcにより事前契約用メタデータを復号し、事業者鍵Kwを含む契約情報を入手するステップと、受信端末は、入手した契約情報に基づき、契約事業者の放送するコンテンツの要求を行うステップと、送出側装置は、暗号化コンテンツの配信と同期させ、有料事業者IDを非暗号化として含み、コンテンツを視聴する際に必要となるコンテンツの暗号鍵Kkを含む必要部分が事業者鍵Kwで暗号化された鍵配信用メタデータと、コンテンツ配信装置位置を含むコンテンツに対する利用制限情報を含む必要部分をコンテンツ鍵Kkで暗号化された蓄積/再生用メタデータとを配信するステップと、受信端末は、暗号化コンテンツと同期させて配信される鍵配信用メタデータを受信し、非暗号化部分に格納されている有料事業者IDにより契約事業者による放送かを判断し、契約する事業者の放送するコンテンツに対する鍵配信用メタデータであると判断した場合、事前契約用メタデータにより配信された事業者鍵Kwにより暗号化部分を復号し、復号された対象契約コードと事前契約用メタデータにより配信された契約コードとによりユーザーの契約形態内で利用可能なコンテンツかを判断し、利用可能であればコンテンツ鍵Kkを受信端末に格納し、同時に受信した蓄積/再生用メタデータの暗号化部分をコンテンツ鍵Kkにより復号し、コンテンツに対する利用制限情報を確認し、ユーザーの利用が可能であれば、蓄積/再生用メタデータに格納されている暗号化コンテンツの配信場所の情報により暗号化コンテンツを受信するステップとを含むデータ配信サービス方法が提供される。

【００１０】

【発明の実施の形態】１．概要

（サービス概要）本総合データ配信サービスとは、見たいコンテンツを見たい時に見たい場所で見られる情報（データ）配信サービスであり、従来のリアルタイム型（放送しているものを視聴する）デジタル放送とは異なり、リアルタイム型に限らず蓄積型の情報配信をも行うサービスである。これにより視聴者が、何時でも好きなときに蓄積されたコンテンツの中から好みのコンテンツを選んで視聴することが可能なニアビデオオンデマンド（NVOD：Near Video On Demand）的なサービスが提供される。また、リムーバブルメディア、本サービスを受信する受信端末に接続される外部機器に直接コンテンツを蓄積させるもしくは、コピーすることによりユーザーの好きな場所でのコンテンツ視聴をも提供する。さらに従来のデジタル放送サービスでは端末単位での契約等の狭い範囲でのコンテンツ利用契約形態のみであったが、本サービスではユーザー個人単位での契約等も可能な広範囲のコンテンツ利用契約形態を提供する。

【００１１】図１に、総合データ配信サービスの受信側の構成図を示す。本総合データ配信サービスの概要として、蓄積型テレビ放送について図１を用い説明する。受信側では、アンテナ２、受信端末３及びテレビ９を備える。蓄積型テレビ放送とは従来のテレビ放送と同様に放送サイド（放送局）から送られてくるコンテンツ１（番組）をアンテナ２（ケーブルでの配信、パッケージでの配信の場合もある）、受信端末３で受信しテレビ９などのモニタ装置にて配信されてくるその瞬間から視聴を行う、ここではリアルタイム型視聴６と呼ぶ場合に加え、従来のビデオデッキ等と同様に一度配信されてきたコンテンツを蓄積媒体４（ハードディスク等の大容量蓄積媒体）に蓄積後視聴する蓄積型視聴８（DVD-RAM等の可搬性に富んだリムーバブルメディア５を蓄積媒体として使用することもある）、蓄積されたコンテンツと配信中のリアルタイム視聴型のコンテンツを合わせて視聴するリアルタイム型＋蓄積型視聴７などのサービスを可能とする情報配信サービスである。

【００１２】（システム概要）図２に、総合データ配信サービスの全体システム構成図を示す。本総合データ配信サービスを行うシステムとしては、衛星放送、地上波放送など電波によるインフラの他にケーブルテレビ、イ

ンターネットなどの通信線を利用したインフラでのサービスが可能であるが、本発明では一例として、図２のような衛星を利用したデジタル衛星放送をインフラとした場合について述べる。

【００１３】総合データ配信サービスが提供されるシステムの概要について図２を用い説明する。本総合データ配信サービスのシステムは送出側１００、受信側２００、送出側１００と受信側２００を結ぶ伝送路である衛星を利用した衛星回線１０、地上回線１１、流通網１２、携帯電話網１３を備える。ここでいう受信側２００とは、必ずしも家庭２０１に設置される受信端末３のみでなく、自動販売機のような公衆端末２０２、コンビニエンスストア等の店舗２０３に設置される端末、移動体である自動車等に搭載される車載端末２０４、携帯端末２０５等も想定する。送出側１００では、コンテンツ１及び制御情報等を制作、管理し受信側２００へ配信する配信センタ、コンテンツの暗号化等に使用する鍵を生成管理する鍵管理センタ、受信側のユーザーの情報を管理する顧客管理センタ、受信側のユーザーからのリクエスト、視聴履歴収集等の地上回線１１、携帯電話２０６を利用した通信を管理する地上回線管理センタ、ユーザー、販売店等に対してDVD等のパッケージメディアによるコンテンツの配信（配達）を行う物流管理センタ等を備える。

【００１４】（サービス内容）次に図２のシステムにおいて行われるサービスについて説明する。本総合データ配信サービスにおけるサービスとしては、例えば、第１に前述したように衛星デジタル回線１０を主に利用しデジタル情報としての、ビデオ、音楽、電子雑誌、ゲーム等の映像、音声、データによる総合データを家庭に設置される受信端末３に向けて配信する家庭向けサービス３００がある。第２に、家庭向けサービス３００と同様に自動販売機２０２、販売店２０３に対しデータを配信し、家庭内で容量的に蓄積しきれないデータ、蓄積をしていないデータのバックアップ、自動販売機、販売店のみで販売可能なデータ等を扱い、例えば販売店でのみ販売可能な電子雑誌を購入し、家庭の受信端末３で視聴を行う自動販売機/販売店向けサービス３０１がある。第３に、車載機器２０４、携帯端末２０５などの外部機器に対し家庭内の受信端末３、もしくは自動販売機２０２、販売店２０３などからコンテンツを携帯し家庭外で視聴を行うことを可能とし、例えば家庭の受信端末に配信された地図データをDVD等のリムーバブルメディア、ICカードを利用することにより車載機器２０４に持ち出し車の中で利用したり、音楽データをメモリカード等のリムーバブルメディア、ICカードを利用することにより持ち出し携帯端末２０５により再生等を行う移動体向けサービス３０２がある。第４に、流通網１２を利用し衛星回線１０で配信出来ないコンテンツ等をCD-ROM、DVD-ROM等のパッケージメディアにより配信を行い、例えばドラマ等のコンテンツを受信端末より予約すると、送出側よりDVD-ROM等で家庭に対しコンテンツを宅配便等で配信するパッケージデリバリサービス３０３がある。第５に、携帯電話２０６等の通信手段を有する外部機器を利用し、送出側を介し家庭内の受信端末をコントロールすることにより例えば、携帯電話２０６の画面上のEPG（電子番組ガイド）より外出先から家庭の受信端末に対して番組予約等を行う携帯電話向けサービス３０４がある。さらに、これらに限定されず、通信インフラ整備に伴い、各種多様の幅広いサービスが可能とされる。本実施の形態では、特に家庭向けサービス３００について説明するが、他のサービスにも適用可能である。

【００１５】（権利保護方式）本総合データ配信サービスとは、直接家庭などにコンテンツを配信し、家庭内等でデジタルデータでの蓄積/コピー/再生を行うことを目的としたサービスであり、これに伴いデータの改ざん、私的利用を超えるコピー、再生等の著作権等の権利に関わる課題が生じるため、コンテンツの著作権、放送事業者、視聴者など各々の権利を保護、管理する必要がある。

【００１６】図３に、総合データ配信サービスにおける権利保護方式の説明図を示す。本総合データ配信サービスにおける権利保護方式について図３を用いて説明する。総合データ配信サービスにおける権利保護方式とは、送出側でコンテンツに対し定義した視聴者へのコンテンツの提示方法、利用条件、コンテンツの暗号鍵等の情報が格納されたメタデータ１８を、暗号化したコンテンツ（暗号化コンテンツ）１７、その他PSI/SI（Program Specific Information/Service Information）等１９と共に配信し、一方、受信端末３側の権利保護機能１６（RMP機能）によりメタデータ１８を解釈し、コンテンツ１７の受信端末３への受信制御、蓄積媒体４、リムーバブルメディア５に対する蓄積制御、コピー制御、暗号/復号制御、ＴＶ９などのモニタ装置に対する提示制御、外部機器１４に対する認証制御、個人を識別するためのICカード１５に対する認証/課金制御等を行う方式である。

【００１７】次に送出側より配信されるPSI/SI１９、コンテンツ１７、メタデータ１８について説明する。PSI/SI１９とは、従来のデジタル放送と同様に、配信中ストリームより必要なデータを取得するためのデータであり、本総合データ配信サービスでは、メタデータ、暗号化コンテンツ等を取得するために利用する。従来のデジタル放送とのサービスの区別は、PSI中のNIT（Network Information Table）内に格納されるサービスリスト記述子、PMT（Program Map Table）内に格納されるストリーム識別記述子等を利用することにより行うこととする。

【００１８】コンテンツ１７は、本総合データ配信サービスにおいて、データの改ざん、不正使用を防ぐために

蓄積媒体４、リムーバブルメディア５等に、基本的に暗号化されたままの状態で蓄積される。また総合データ配信サービスにおけるコンテンツ１７とは、概念的なものであり一定の物理量を示す単位ではなく、送出側の意図する単位で指定可能であり、指定した物理量をメタデータに記すことにより受信端末はコンテンツを認識可能となる。コンテンツは、例えば、また従来のデジタル放送と同様なチャンネルを指定すれば視聴可能な動画による映像系コンテンツと、主に蓄積したのち視聴することを主眼としたデータ系のコンテンツに分けられる。

【００１９】図５０に、映像系及びデータ系コンテンツを構成するデータの説明図の一例を示す。本総合データ配信サービスでは、コンテンツを構成するデータ群の各データをエレメントと呼ぶ。よってコンテンツは１つあるいは複数エレメントより構成されるものとなる。メタデータ１８とは、本総合データ配信サービスにおいて、例えば、送出側である放送事業者の意図する単位で指定されたコンテンツに対して付与されるコンテンツの内容、構成等の検索等に利用される一般的な情報、著作権者及び関連する権利の保護を送出側で定義した視聴者へのコンテンツ提示方法、利用条件等の情報を含む。メタデータは、これらの情報により端末を制御し、権利保護を可能とする。よって、メタデータにはコンテンツと同様、保護すべき情報が含まれるため、一部を暗号化して配信を行い、蓄積時も暗号化されたままの状態で蓄積される。また、メタデータは配信タイミング、内容により、事前契約用メタデータ、EPG用メタデータ、蓄積／再生用メタデータ、鍵配信用メタデータに分類される。

【００２０】事前契約用メタデータは、有料放送事業者毎に固有の鍵である事業者鍵や、契約した事業者の放送する番組の全てが視聴可能か、一部が視聴可能か等を受信端末側で解釈するための契約コード等が格納され、ユーザー個人宛にコンテンツの配信とは非同期に配信される。EPG用メタデータは、受信端末側で配信予定のコンテンツの確認、視聴/蓄積予約を行うために必要となるコンテンツの名称、内容、放送予定日などの情報が格納され、受信端末を使用するユーザーの区別なく対象となるコンテンツの配信以前に全受信端末に向け配信され、主に受信端末のEPG表示、視聴/蓄積予約等を行うためのものである。蓄積/再生用メタデータは、コンテンツの受信、蓄積、コンテンツに対する視聴契約を行うための情報が格納され、受信端末を使用するユーザーの区別なく全受信端末に向け対象となるコンテンツの配信と同期させ配信される。鍵配信用メタデータは、コンテンツの暗号化を行った鍵の情報が格納され、蓄積/再生用メタデータと同様に対象となるコンテンツの配信と同期させ配信される。メタデータリストは、PSI/SIと共に利用することにより蓄積したEPG用メタデータの更新を行うための情報、配信中ストリーム群より必要なデータを取得するための情報が格納され、受信端末を使用するユーザーの区別なく全受信端末に向け常時配信される。システム鍵更新用メタデータは、端末内に予め格納されているシステム全体で共通の鍵を更新するための情報が格納され、受信端末を使用するユーザーの区別なく全受信端末に向けコンテンツの配信とは非同期に配信される。

【００２１】（暗号化方式）次に本総合データ配信サービスにおけるコンテンツ、メタデータの暗号化方式について説明する。本総合データ配信サービスにおけるコンテンツ、メタデータの暗号化方式は、暗号化コンテンツ、暗号化メタデータを復号せずに蓄積するため、従来のデジタル放送における配信時に暗号化を行う方式とは異なり、コンテンツ、メタデータの生成時に暗号化を行う方式である。

【００２２】図４に、総合データ配信サービスと既存サービスの暗号化方式比較の説明図を示す。本総合データ配信サービスにおける暗号化方式と従来のデジタル放送における暗号化方式の比較を図４を用いて説明する。従来方式では、コンテンツを生成２０し、その生成されたコンテンツを暗号化する前に配信時のデータ形態であるTSP２１を形成するため、ブロック分けし、TSPのペイロード部分２２にブロック分けしたコンテンツの一部２３を格納し、その後TSPのペイロード部分を暗号化２４するため、受信端末側でコンテンツを組み立てる際に、ペイロード部分を復号する必要がある。一方、本総合データ配信サービスにおける暗号化方式の場合では、送信側で、コンテンツの生成２０後にコンテンツの暗号化２５を行い、暗号化されたコンテンツをブロック分けし、TSPのペイロード部分２２にブロック分けした暗号化コンテンツの一部のブロック２６を格納し配信するため、受信端末側でコンテンツを組み立てる場合にペイロード部分を復号せずに組み立て可能となり、送出側で暗号化されたままの状態でのコンテンツ、メタデータの蓄積が可能となる。

【００２３】（コンテンツ及びメタデータの暗号化方式）図５に、コンテンツの暗号化方式の説明図を示す。また、図６に、メタデータの暗号化方式の説明図を示す。次にコンテンツ、メタデータそれぞれの暗号化イメージについてそれぞれ図５、図６を用いて説明する。本総合データ配信サービスにおけるコンテンツの暗号化は、映像系コンテンツ２７、データ系コンテンツ２８の種別に関係なく各コンテンツを構成する各エレメント毎に暗号化を行う。例えば映像系コンテンツ２７がMPEG2-Video(PES)２９、MPEG2-AAC(PES)３０の２エレメントから構成されている場合、それぞれのエレメント毎にデータ全てに暗号化を行い、暗号化エレメント３１、３２を生成する。このとき暗号化を行うための暗号鍵３３はコンテンツ内では共通な暗号鍵Kklを使用する。本総合データ配信サービスではコンテンツ毎に割り当てられるこの暗号鍵３３をコンテンツ鍵Kklと呼ぶ。よって、映像系コンテンツ２７とは別のコンテンツであるデータ系コ

ンテンツ２８を構成する各エレメントは別の暗号鍵３４で暗号化される。このとき暗号鍵３４には、同様に、コンテンツ内で共通な鍵Kk2を使用する。なお、コンテンツ鍵Kkは、コンテンツ鍵全体の総称である。

【００２４】本総合データ配信サービスにおけるメタデータの暗号化は、コンテンツの暗号化とは異なり暗号化が必要なメタデータの全体に暗号化を行うのではなく、図６のように暗号化が必要な部分３５のみ抽出し暗号化を行い、暗号化したデータの容量３６等の情報を加えた暗号化データ３７を生成する。また、本総合データ配信サービスでは運用によりこの暗号化データ３７を、暗号化を行わないメタデータ３８に再度埋め込み配信する場合と、別ファイルとして配信する場合とが可能である。図５１に、本総合データ配信サービスにおいてコンテンツ、前述した各メタデータを暗号化する際に使用する暗号鍵、暗号鍵についての説明図を示す。

【００２５】（限定受信方式）図７に、総合データ配信サービスにおける限定受信方式の説明図を示す。次に、本総合データ配信サービスにおいて有料放送等のコンテンツを放送事業者と契約のあるユーザーにのみ受信/蓄積させる限定受信の方式について図７を用いて説明する。本総合データ配信サービスにおける限定受信方式とは、従来のデジタル放送で使用される方式による端末毎にチャンネル単位、番組単位に行う方式とは異なり、メタデータを利用することにより端末を利用するユーザー毎に、コンテンツ単位の限定受信を可能とする。コンテンツ単位とは前述の通り、放送事業者の意図する単位であるため最小単位はエレメント単位となり、番組を構成するワンシーン等の細かい単位での限定受信が可能となる。本総合データ配信サービスにおける方式は、事前契約用メタデータ、鍵配信用メタデータにより限定受信を行う。

【００２６】まず受信側２００のユーザーが有料事業者に対し端末ID、個人ID、契約したいチャンネル、番組、コンテンツ等の契約要求３９を送出側１００に通知する。送出側１００ではユーザーより通知された契約要求より事前契約用メタデータを生成し、契約情報等の保護の必要な部分を受信端末毎に固有の端末鍵Kmcで暗号化を行い受信側２００にユーザー毎に配信する４５。受信側２００の受信端末では、事前契約用メタデータ４０の非暗号化部分に格納されている端末ID、個人IDにより端末を使用するユーザー宛の情報かを判断し、使用ユーザー宛のIDが格納されている場合は、端末内に予め格納されている端末鍵Kmc４３により事前契約用メタデータを復号し、有料事業者ID、事業者毎に固有の事業者鍵Kw４４、契約コード等により構成される契約情報を入手する。契約情報を入手したユーザーは、次に契約事業者の放送するコンテンツ１７の要求４６を行う。送出側１００では、暗号化コンテンツ１７の配信と同期させコンテンツを視聴する際に必要となるコンテンツの暗号鍵Kk３３が格納され、必要部分を事業者鍵Kw４４で暗号化された鍵配信用メタデータ４１を全端末に配信する。また、送信側１００では、コンテンツに対する利用制限情報等が格納され、必要部分がコンテンツ鍵Kk３３で暗号化された蓄積/再生用メタデータ４２を全端末に配信する。受信端末はコンテンツと同時に配信されている鍵配信用メタデータ４１を受信し、非暗号化部分に格納されている有料事業者IDにより契約事業者による放送かを判断し、契約する事業者の放送するコンテンツに対する鍵配信用メタデータ４１であると判断した場合、事前契約用４０メタデータにより配信された事業者鍵Kwにより暗号化部分を復号し、復号された対象契約コードと事前契約用メタデータ４０により配信された契約コードによりユーザーの契約形態内で利用可能なコンテンツかを判断する。ここで、利用可能であればコンテンツ鍵Kk３３を受信端末に格納し、同時に受信した蓄積/再生用メタデータ４２の暗号化部分をコンテンツ鍵Kk３３により復号し、コンテンツに対する年齢制限等の利用制限情報を確認し、ユーザーの利用が可能であれば、蓄積/再生用メタデータ４２に格納されている暗号化コンテンツ１７の配信場所の情報により暗号化コンテンツ１７の受信が可能となる。本総合データ配信サービスでは上記の方式により限定受信を可能とする。

【００２７】２．課金方式

次に本総合データ配信サービスにおける課金方式について説明する。本総合データ配信サービスでは、事前契約に対する課金と、コンテンツの視聴時に対する課金の大きく２通りに分けられる。

【００２８】（事前契約に対する課金）図８に、事前契約による課金方式の説明図を示す。まず事前契約に対する課金について図８を用いて説明する。事前契約に対する課金とは、送出側１００で予めユーザー登録４７により得た顧客情報を元に課金を行うため、ユーザーのコンテンツ視聴の有無に関係せずに定額の課金が可能となる課金方式である。受信端末３を購入したユーザーは、送出側１００に対し、端末ＩＤ、個人ID、契約したい事業者、契約形態、契約期間等の情報と共に決済先の銀行口座等４８の情報を葉書や電話等により通知する。送出側１００ではこれらの情報を元に顧客情報を生成管理し、契約した事業者の鍵、契約形態を示す契約コード、契約の有効期限等を格納した事前契約用メタデータ４０を生成し契約ユーザーの受信端末３に向け配信し、ユーザーの指定した口座等４８より一定期間のコンテンツ利用契約に対する課金を行う。事前契約メタデータ４０を受信したユーザーは、格納されている有効期限の範囲で契約した事業者のコンテンツの利用が可能となる。以上が本総合データ配信サービスにおける事前契約に対する課金フローである。

【００２９】（視聴契約に対する課金）次に視聴契約に対する課金について説明する。本総合データ配信サービ

スにおける視聴契約に対する課金方式では、地上回線等の受信端末より送出側の上り回線を前提とした課金方式と、上り回線を前提としない課金方式に分けられる。

【００３０】（上り回線を前提としない課金方式）図９に、上り回線を必要としない視聴契約に対する課金方式の説明図を示す。まず地上回線等の上り回線を前提としない課金方式について図９を用いて説明する。上り回線を前提としない課金方式とは、一定ポイントの利用料を事前契約の場合と同様に事前に支払い、そのポイントの範囲でコンテンツの視聴を行う方式である。但し、一定ポイントを超える場合は追加ポイントをその都度契約可能とする。具体的な手段としては、事前契約に対する課金と同様に、受信端末を購入したユーザーが端末ID、個人ID、契約したい事業者、契約形態、決済先の銀行口座４８等を送出側１００に通知し契約を行う際に一定期間に対する契約ではなく、コンテンツを利用するためのポイント数４９を通知し契約を行う。送出側１００では、これらの情報を元に顧客情報を生成管理し、契約の有効期限に関する情報の代わりに許諾するポイント数の情報を事前契約用メタデータ４０に格納し契約ユーザーの受信端末３に配信する。また送出側１００ではコンテンツ１７を配信する際に同期させ配信させる蓄積/再生用メタデータ４２にコンテンツを利用する際に必要となるポイント数の情報を格納し配信する。受信端末３ではコンテンツを利用する際に、事前契約用メタデータ４０により配信されたポイント数より蓄積/再生用メタデータ４２に格納されている必要ポイント数を減算し、コンテンツの再生を行うため、事前契約用メタデータ４０で配信されたポイント数の範囲でのコンテンツの視聴が可能となる。事前契約用メタデータ４０で配信されたポイント数がなくなった場合、ユーザーは再度送出側１００と契約し、事前契約用メタデータ４０を受信することによりポイントの補充が可能となる。送出側では、ユーザーに許諾したポイント数に応じて事前に通知された指定口座等４８よりの課金が行えるため、ユーザーのコンテンツの視聴に応じた課金が可能となる。事前契約用メタデータ４０により配信されるポイント数は、基本的にICカード内に格納するが、受信端末を利用するユーザーグループに対するポイント等の場合においては受信端末内に格納することも可能である。

【００３１】（上り回線を前提とした課金方式）次に地上回線１１等の上り回線を受信端末３に接続することを前提とした課金方式について説明する。本総合データ配信サービスにおける前項のポイントに対する課金方法の拡張として、ポイントの申し込み、ポイント追加等を受信端末３に接続された地上回線１１等によりオンラインで可能にする方式と、実際に受信端末側でコンテンツを利用した際の課金情報５０が送出側１００に地上回線１１等を通じて送られ、その情報を元に課金を行う方式が存在する。

【００３２】図１０に、上り回線を使用したオンライン課金方式の説明図を示す。ここでは後者の課金情報５０による方式について図１０を用いて説明する。オンラインで課金情報５０を送出側１００に送り課金を行うための具体的な手段としては、前述した課金方式と同様に受信端末３を購入したユーザーが端末ID、個人ID、契約したい事業者、契約形態、決済先の口座４８等を送出側１００に通知する際に、一定期間、一定ポイント数に対する契約ではなく、オンラインでのコンテンツの視聴に対する課金情報５０を送るための契約を行う。本総合データ配信サービスでは、この契約をオンラインPPV許諾契約と呼ぶ。送出側１００ではこれらの情報を元に顧客情報を生成管理し、契約の有効期限、許諾ポイント数等の情報の代わりにオンラインPPV許諾として、課金情報送信時の送信先の情報等を事前契約用メタデータ４０に格納し契約ユーザーの受信端末３に配信する。また送出側１００ではコンテンツ１７を配信する際に同期させ配信させる蓄積/再生用メタデータ４２にコンテンツを利用する際に必要となる利用時の料金などの課金情報５０を生成する元となる情報を格納し配信する。受信端末ではコンテンツを利用する際に、蓄積/再生用メタデータ４０に格納された課金情報５０を生成するための元となる情報に対し利用ユーザーのID等の情報を加え、事前契約用メタデータ４０により指定された送信先に対し地上回線を利用し送信する。これにより送出側１００では契約ユーザーの受信端末３より送信された課金情報５０内の料金を事前に登録された指定口座等４８よりユーザーのコンテンツ視聴量に応じ課金可能となる。

【００３３】３．サービスフロー

図１１に、総合データ配信サービスにおけるサービスの流れの説明図を示す。次に本総合データ配信サービスにおけるサービスの流れについて図１１を用いて説明する。本総合データ配信サービスは、例えば、受信端末３購入時に添付される葉書もしくは電話等を利用したユーザー登録時の事前契約フロー１０５、送出側１００におけるコンテンツ生成１０２、メタデータ生成１０３から配信１０４までの送出側フロー１０１、コンテンツの受信、再生等の受信側フロー３３１を含む。

【００３４】（事前契約フロー）図１２に、事前契約におけるサービスフローの説明図を示す。以下に、事前契約におけるサービスフローを図１２を用いて説明する。総合データ配信サービスにおける事前契約フロー１０５とは、送出側１００におけるサービス受信ユーザ１０６の顧客情報管理１０７を行うことを目的とする。総合データ配信サービスでは有料の蓄積型コンテンツをメインとしたサービスであるため、ユーザーはコンテンツの視聴契約を行うためのICカード１５が必要となり、そのICカード１５をユーザーが取得する手段が事前契約である。前述の限定受信方式、課金方式で説明した通り、受信側２００のユーザー１０６は、端末購入時に添付され

る葉書もしくは電話等によりユーザー１０６の氏名、住所、有料放送視聴時等の決済先である銀行口座等のユーザー個人に関する個人情報および、視聴したい有料サービス、契約形態等を端末ID等の受信端末を識別する情報と共に送出側１００に登録する。送出側１００では、ユーザー登録された個人情報、契約情報、受信端末３を識別するための端末ID等の情報を元にユーザーに対し個人IDを割り振り顧客情報を生成管理１０７する。また、送信側１００では、この顧客情報を元にICカード１５に対し割り振った個人ID等の情報を格納し、ユーザー１０６に対しそれを配布し、受信端末３、配布したICカード１５に対してICカードを有するユーザー１０６が契約を行った事業者の鍵、契約形態を示す契約コード等の情報が格納された事前契約用メタデータ４０を配信する。ユーザー１０６は契約したコンテンツの利用が可能となり、送出側１００では契約ユーザーの顧客情報の管理が可能となる。

【００３５】（送出側フロー）図１３に、送出側におけるサービスフローの説明図を示す。以下に、送出側のサービスフローについて図１３を用いて説明する。総合データ配信サービスにおける送出側のサービスフローとは、例えば、コンテンツの生成１０２、番組編成２０８、コンテンツの暗号化２０９、配信フォーマット化２１２、PSI/SI生成２１０、メタデータ生成１０３、メタデータ暗号化２１１、配信１０４を含む。

【００３６】コンテンツ生成１０２とは、映像/音声/データの各エレメントよりコンテンツ１を生成することである。番組編成２０８とは、生成したコンテンツの１つあるいは複数を組み合わせることにより放送番組を制作することである。コンテンツの暗号化２０９は、番組化した各コンテンツに含まれるエレメントをコンテンツ毎の鍵であるコンテンツ鍵Kkにより暗号化し暗号化コンテンツ１７を生成することである。配信フォーマット化２１２は、暗号化コンテンツ１７、暗号化されたメタデータをエレメントの種別により配信時のデータフォーマットであるTSP化することである。PSI/SI生成２１０とは番組編成２０８を行うことにより生成される番組の運行情報等を元にPSI/SIテーブル１９を生成することである。メタデータ生成１０３とは、コンテンツ生成１０２、番組編成２０８時のコンテンツ、番組に対するタイトル、内容、構成、利用制限情報等や、コンテンツ暗号化２０９における暗号方式、暗号鍵等の情報、配信フォーッマト化２１２した際の伝送路における配信位置等の情報よりメタデータリスト２５０、EPG用メタデータ２５１、蓄積/再生用メタデータ２５２、鍵配信用メタデータ２５３の各メタデータを生成することである。メタデータ暗号化２１１とは、メタデータ生成１０３により生成された各メタデータの保護が必要な部分に対し暗号化を行うことで、暗号化EPG用メタデータ２５４、暗号化蓄積/再生用メタデータ２５５、暗号化鍵配信用メタデータ２５６を生成することである。配信２１２とは、PSI/SI、各メタデータ、暗号化コンテンツを多重化し受信側に配信することである。

【００３７】（受信側フロー）図１４に、受信側におけるサービスフローの説明図を示す。総合データ配信サービスにおける受信側のサービスフローとは、例えば、予約３３２、コンテンツ受信/蓄積３３３、視聴契約３３４、再生３３５を含む。予約３３２とは、送出側１００より配信されるEPG用メタデータ２５４を利用し、希望するコンテンツの予約を行うことである。コンテンツ受信/蓄積３３３とは、予約した情報を元にコンテンツ配信時刻に蓄積/再生用メタデータ２５５、鍵配信用メタデータ２５６、暗号化コンテンツ１７を受信し、蓄積/再生用メタデータ２５５、暗号化コンテンツ１７を蓄積することである。視聴契約３３４とは、蓄積された蓄積/再生用メタデータの利用制限情報、ICカード１５内の個人情報、契約情報等によりコンテンツの視聴契約を行うことである。再生３３５とは、視聴契約を行った情報をもとにコンテンツの再生許可等を判断し、暗号化コンテンツ１７の復号を行った後、コンテンツの再生を行うことである。

【００３８】４．送出側システム

次にこれらのサービスフローを実現させるための送出側のシステムについて説明する。

送出側システム構成

図１５に、送出側システム全体の構成図を示す。総合データ配信サービスにおける送出側システムの全体構成を図１５を用いて説明する。送出側システムは前述の通りコンテンツやメタデータの生成、暗号化、配信を行う配信センタ２２０、総合データ配信サービスシステムで使用する鍵や、IDを生成管理する鍵管理センタ２４０、ユーザー登録情報により各ユーザーの個人情報、契約情報等の顧客情報の生成管理を行う顧客管理センタ２６０、ユーザーからの視聴履歴情報/課金情報、リクエスト等の双方向通信サービス利用時の地上回線１１による接続の管理を行う地上回線管理センタ２１４、ユーザーや、販売店に対する商品等の配送など流通網１２を利用した物流の管理を行う物流管理センタ２１３等を備える。本発明では総合データ配信サービスを実現する上で特に重要となる配信センタ２２０、鍵管理センタ２４０、顧客管理センタ２６０について詳細に説明する。

【００３９】（１）配信センタ構成

図１６に、配信センタ内の構成図を示す。配信センタ２２０内の構成を図１６を用いて説明する。配信センタ２２０はコンテンツの制作を行うオーサリングシステム２２１、オーサリングシステム２２１で制作されたコンテンツより番組を編成し、運行スケジュール等を生成管理する番組構成管理システム２２２、オーサリングシステム２２１、番組構成管理システム２２２よりのコンテンツ生成時、番組編成時に生成されるコンテンツ及び番組

19

のタイトル、構成等の情報を元に各メタデータを生成するメタデータ生成装置２２３、番組構成管理システム２２２で生成される運行スケジュール等を元にPSI/SIを生成するPSI/SI生成装置２２４、番組構成管理システム２２２により番組編成されたコンテンツ内の各エレメントを暗号化するコンテンツ暗号化装置２２５、メタデータ生成装置２２３により生成されたメタデータの暗号化を行うメタデータ暗号化装置２２６、PSI/SI装置２２４、コンテンツ暗号化装置２２５、メタデータ暗号化装置２２６等より入力された情報を多重化し配信可能なフォーマットに変換する送出系システム２２７を備える。以下これら各構成について説明する。

【００４０】（オーサリングシステム）図１７に、オーサリングシステム内の構成図を示す。コンテンツを生成するオーサリングシステム２２１について図１７を用いて説明する。オーサリングシステム２２１とはコンテンツ１の生成および管理を行い、完成したコンテンツ、コンテンツを生成する際に生成されるコンテンツに関するタイトル、内容、コンテンツ内の構成等の情報が格納された関連ファイル２３３を番組構成管理システム２２２に受け渡すシステムである。オーサリングシステム２２１の構成としては、映像、音声、データのエレメントを制作編集する映像オーサリングツール２２８、音声オーサリングツール２２９、データオーサリングツール２３０、各オーサリングツールより出力されるエレメントよりコンテンツ１を構成し、関連ファイル２３３を生成するコンテンツ構成装置２３１、コンテンツ構成装置により生成されたコンテンツ、関連ファイル２３３を蓄積管理するためのコンテンツ管理サーバ２３２を備える。

【００４１】映像オーサリングツール２２８、音声オーサリングツール２２９、データオーサリングツール２３０、の各オーサリングツールは、VHSビデオ、レーザーディスク（登録商標）、写真等のアナログの素材入力２３４に対しデジタル化するビデオキャプチャ、スキャナー等の機能、DAT、CD、DVD等のデジタルの素材入力２３４に対して受信側の受信端末が表示可能なフォーマットへの変換機能、各デジタル素材の編集機能、コンテンツ構成装置２３１に対して制作、編集を行った各エレメントのデジタル出力機能等を有する。コンテンツ構成装置２３１は、各オーサリングツールより出力される１つあるいは複数エレメントよりコンテンツ１を構成し、同時にコンテンツ名、コンテンツID、コンテンツの内容、ジャンル、コピー制限、対象年齢、著作権等の利用制限情報、構成するエレメントのデータ形式、容量等の情報を入力することにより関連ファイル２３３を生成しコンテンツ管理サーバ２３２に蓄積する機能を有する。コンテンツ管理サーバ２３２は、コンテンツの完成を番組構成管理システム２２２に対し通知し、番組構成管理システム２２２よりコンテンツ、関連ファイル２３３の転送要求が起こった場合、番組構成管理システム２２２に対し要求されたコンテンツ１、関連ファイル２３３を受け渡す機能を有する。但し、コンテンツ管理サーバ２３２は番組構成管理システム２２２より転送要求が無い場合においても強制的に番組構成管理システムに対しコンテンツ１、関連ファイル２３３を受け渡す機能をも有する。

20

【００４２】（番組構成管理システム）図１８に、番組構成管理システム内の構成図を示す。次に番組構成管理システム２２２について図１８を用いて説明する。番組構成管理システム２２２とは、オーサリングシステム２２１で生成されたコンテンツより番組を構成し、構成した番組に対する運行スケジュール等を生成管理することにより番組を編成するシステムである。番組構成管理システム２２２は、オーサリングシステム２２１内のコンテンツ管理サーバ２３２より入力されるコンテンツ１より番組を構成する番組構成装置２３５、構成された番組に対し運行スケジュール２３８を生成し、割り当てる番組運行スケジュール生成装置２３６、番組化されたコンテンツ群、それに対応する関連ファイル群、運行スケジュールを蓄積管理する番組管理サーバ２３７を備える。なお、図１７、１８のコンテンツ生成におけるコンテンツに関連する情報を纏めたファイルをコンテンツ関連情報と総称し、それを記憶したファイルが関連ファイル２３３である。

【００４３】番組構成装置２３５とは、コンテンツ管理サーバ２３２より１つあるいは複数のコンテンツ１、関連ファイル２３３より番組を構成し、番組としてのコンテンツ群、番組に対する情報、例えば番組のタイトル、番組のID、番組の内容、ジャンル、放送する事業者のID、契約に関する情報、課金に関する情報、番組内におけるコンテンツの構成等の情報をコンテンツ管理サーバ２３２より入力された関連ファイル２３３に追加し、番組管理サーバ２３７に対し蓄積する機能を有する。番組運行スケジュール生成装置２３６は、番組管理サーバ２３７に蓄積された番組に対し、放送日時、チャンネル等の放送場所に関する情報等を割り当て、運行スケジュール２３８を生成し番組管理サーバ２３７に蓄積する機能を有する。番組管理サーバ２３７は、番組構成装置２３５、番組運行スケジュール生成装置２３６より入力されたコンテンツ群１、関連ファイル群２３３、運行スケジュール２３８等を蓄積管理し、運行スケジュール２３８の情報を元に、メタデータ生成装置２２３、PSI/SI生成装置２２４に対し運行スケジュール２３８、関連ファイル群２３３を入力し、コンテンツ暗号化装置２２５に対しメタデータ生成装置２２３、PSI/SI生成装置２２４に入力した番組情報に対応するコンテンツ群及びコンテンツのID群を入力する機能を有する。

【００４４】（PSI/SI生成装置）図１９に、PSI/SI生成装置の説明図を示す。PSI/SI生成装置２２４について図１９を用いて説明する。PSI/SI生成装置２２４とは、番組構成管理システム２２２内の番組管理サーバ２３７よ

り入力される運行スケジュール２３８、関連ファイル群２３３よりMPEG2-Systemに準拠したPSI/SIの各テーブルを生成し、運行スケジュールの情報を元に送出系システム２２７に対しTSP化した各PSI/SIテーブルを入力する機能を有する。

【００４５】（メタデータ生成装置）図２０に、メタデータ生成装置の説明図を示す。次にメタデータ生成装置２２３について図２０を用い説明する。メタデータ生成装置２２３とは、番組構成管理システム２２２内の番組管理サーバ２３７より入力される関連ファイル群、運行スケジュール、鍵管理センタ２４０に対しコンテンツのIDを受け渡すことにより得られるコンテンツ鍵Kk、送出系システム２２７より入力されるコンテンツ等の伝送路における配信位置情報等を元に、メタデータリスト２５０、EPG用メタデータ２５１、鍵配信用メタデータ２５３、蓄積/再生用メタデータ２５２を生成し、メタデータリストを送出系システム２２７に出力し、その他のメタデータをメタデータ暗号化装置２２６に出力する機能を有する。送出系システムより入力されるコンテンツ等の伝送路における配信位置情報は、送出系システム２２７側の装置により配信位置であるモジュールの指定等が可能であれば必要としない場合もある。

【００４６】（コンテンツ暗号化装置）図２１に、コンテンツ暗号化装置の説明図を示す。本システムにおけるコンテンツ暗号化装置２２５について図２１を用いて説明する。コンテンツ暗号化装置２２５とは、番組構成管理システム２２２内の番組管理サーバ２３７より入力されるコンテンツ群、ID（コンテンツID）群に基づき、番組管理サーバ２３７より入力されたID（コンテンツID）を鍵管理センタ２４０に通知し、該当するコンテンツ鍵Kkを受け取り、また、コンテンツ鍵Kkにより対応するコンテンツ内の各エレメントを前述のコンテンツ暗号化方式の通り暗号化し、生成した暗号化コンテンツを送出系システム２２７に対し出力する機能を有する。

【００４７】（メタデータ暗号化装置）図２２に、メタデータ暗号化装置の説明図を示す。次にメタデータ暗号化装置２２６について図２２を用い説明する。メタデータ暗号化装置２２６とは、メタデータ生成装置２２３より入力されるEPG用メタデータ２５１、蓄積/再生用メタデータ２５２、鍵配信用メタデータ２５３、顧客管理センタ２６０より入力される事前契約用メタデータ２５９を鍵管理センタ２４０内より入力される暗号鍵情報により暗号化し、生成された暗号化メタデータを送出系システム２２７に対し出力する機能を有する。

【００４８】各メタデータの暗号化方式について、以下に説明する。EPG用メタデータ２５１については、鍵管理センタ２４０に対しEPG用メタデータ２５１に格納されたシステムIDを受け渡すことにより得られる全受信端末に共通したシステム鍵Ksy２６４により必要部分に対し暗号化が行われる。蓄積/再生用メタデータ２５２については、鍵管理センタ２４０に対し蓄積/再生用メタデータ２５２に格納されたコンテンツIDを受け渡すことにより得られるコンテンツ毎に固有のコンテンツ鍵Kk３３により必要部分に対し暗号化が行われる。鍵配信用メタデータ２５３については、メタデータ内に格納されているIDを次のように暗号化する。すなわち、無料コンテンツに対する鍵配信用メタデータ２５７であれば、システムIDを、鍵管理センタ２４０に受け渡すことにより得られるシステム鍵Ksy２６４により、必要部分に対し暗号化する。また、有料コンテンツに対する鍵配信用メタデータ２５８であれば、事業者IDを、事業者鍵Kw４４により、それぞれ必要部分に対し暗号化する。事前契約用メタデータ２５９については、鍵管理センタ２４０に対し事前契約用メタデータ２５９内に格納された端末IDを受け渡すことにより得られる端末鍵Kmc４３により必要部分に暗号化が行われる。

【００４９】よって送出系システム２２７に対しては生成された暗号化EPG用メタデータ２５４、暗号化蓄積/再生用メタデータ２５５、暗号化鍵配信用メタデータ（無料）２６１、暗号化鍵配信用メタデータ（有料）２６２、暗号化事前契約用メタデータ２６３が出力されることとなる。

【００５０】（送出系システム）図２３に、送出系システム内の構成図を示す。以下に、総合データ配信サービスにおける送出系システム２２７について図２３を用いて説明する。送出系システム２２７とは、PSI/SI生成装置２２４、コンテンツ暗号化装置２２５、メタデータ暗号化装置２２６、メタデータ生成装置２２３より入力されるPSI/SI、暗号化コンテンツ、メタデータ等のデータを、受信端末３に対し配信可能なデータに組み立てるシステムである。送出系システム２２７は、カルーセル生成装置２３９、パケタイザ２４１、多重化装置（MUX）２４２、受託放送設備２４３を備える。カルーセル生成装置２３９とは、コンテンツ暗号化装置２２５より入力されるデータ系の暗号化コンテンツ、メタデータ暗号化装置より入力される暗号化された各メタデータ、メタデータ生成装置より入力されるメタデータリストよりMPEG2-systemにおけるデータカルーセルを生成するために各データをモジュール化したのちDII、DDB化し、パケタイザ２４１に対し出力する機能を有する。パケタイザ２４１とは、コンテンツ暗号化装置より入力されるMPEG2-Video PES、MPEG2-Audio PES等の映像系の暗号化コンテンツ、カルーセル生成装置より入力されるDII、DDB等のデータをTSP形式のデータに分割し多重化装置（MUX）２４２に対し出力する機能を有する。多重化装置（MUX）２４２とは、PSI/SI生成装置２２４、パケタイザ２４１より入力されるTSPに対し送出レート等の条件により多重化を行いTSを生成し、受託放送設備２４３に出力する機能を有する。受託放送設備２４３とは、多重化装置（MUX）２４２より入力される複数TSをさらに多重化し、受

信端末３に対して配信可能なデータ形体とし送信アンテナより配信を行う機能を有する。以上が本総合データ配信サービスにおける配信センタ２２０内の構成および各構成装置の機能及びデータ生成フローである。

【００５１】（２）鍵管理センタ構成

図２４に、鍵管理センタ内の構成図を示す。次に鍵管理センタ２４０について図２４を用いて説明する。鍵管理センタ２４０とは、配信センタ２２０、顧客管理センタ２６０より登録される各IDに対する暗号鍵を生成し、各センタからの暗号鍵の要求に対して暗号鍵を受け渡すシステムである。鍵管理センタ２４０は、鍵生成装置２４４、鍵管理サーバ２４５を備える。

【００５２】（鍵生成装置）図２５に、鍵生成装置の説明図を示す。次に鍵管理センタ２４０における鍵生成装置２４４について図２５を用いて説明する。鍵生成装置２４４とは、配信センタ２２０内のメタデータ生成装置２２３より入力される複数のコンテンツID２４６よりそれぞれのIDに対応するコンテンツの暗号鍵であるコンテンツ鍵Kk３３を生成し、生成したコンテンツ鍵Kk３３をコンテンツID２４６と共に鍵管理サーバ２４５に対し出力する機能を有する。また、システム鍵Ksy２６４、事業者鍵Kw４４、端末鍵Kmc４３、個人鍵Km２６５については鍵生成装置２４４内で各暗号鍵に対するIDであるシステムID２４７、事業者ID２４８、端末ID２４９、個人ID２７０を直接指定することにより生成し、各IDと共に鍵管理サーバ２４５に対し出力する。

【００５３】（鍵管理サーバ）図２６に、鍵管理サーバの説明図を示す。次に鍵管理サーバ２４５について図２６を用いて説明する。鍵管理サーバ２４５とは、鍵生成装置２４４により生成された鍵及びIDを管理し、配信センタ２２０内のコンテンツ暗号化装置２２５、メタデータ暗号化装置２２６、メタデータ生成装置２２３、顧客管理センタ２６０内の顧客情報管理サーバ２６７よりの暗号鍵の要求に対し対応する暗号鍵を受け渡す機能を有する。例えば配信センタ２２０内のコンテンツ暗号化装置２２５より暗号鍵の要求としてコンテンツIDを受け渡された場合は、コンテンツIDに対応する暗号鍵であるコンテンツ鍵Kkを受け渡す機能である。

【００５４】（３）顧客管理センタ構成

図２７に、顧客管理センタ内の構成図を示す。次に本総合データ配信サービスシステムにおける顧客管理センタについて図２７を用いて説明する。顧客管理センタ２６０とは、ユーザー１０６からのユーザー登録情報を元に顧客情報を生成し、鍵管理センタ２４０より受け渡される暗号鍵等の情報によりICカード、事前契約用メタデータを生成し、ICカードをユーザー１０６に配布し、事前契約用メタデータを配信センタ２２０に受け渡すシステムである。顧客管理センタ２００は、顧客情報生成システム２６６、顧客情報管理システム２７１を備える。

【００５５】（顧客情報生成システム）図２８に、顧客情報生成システム内の構成図を示す。顧客管理センタ２６０における顧客情報生成システム２６６について図２８を用いて説明する。顧客情報生成システム２６６とは、ユーザー１０６が端末購入時に添付される葉書もしくは電話にて事前契約等のユーザー登録を行った情報より顧客情報を生成し、顧客情報管理システム２７１に対し出力するシステムであり、ユーザーI/F２６８、顧客情報生成装置２６９を備える。ユーザーI/F２６８とは、ユーザーからの葉書、電話等によるユーザー登録情報を受付け、登録された情報を電子化する機能を有する。顧客情報生成装置２６９とは、ユーザーI/F２６８により電子化されたユーザー登録情報を顧客情報管理システム２７１が認識可能なデータ形式である顧客情報に編集し、顧客情報管理システム２７１に対し出力する機能を有する。

【００５６】（顧客情報管理システム）図２９に、顧客情報管理システム内の構成図を示す。顧客情報管理システム２７１とは、顧客情報生成システム２６６により入力される顧客情報を元に鍵管理センタ内の鍵管理サーバ２４５に対し個人ID２７０、個人鍵２６５等を要求し、受け取った個人ID２７０、個人鍵２６５等を利用し、事前契約用メタデータ４０、ICカード１５等を生成するシステムである。顧客情報管理システム２７１は、顧客情報管理サーバ２６７、ICカード生成装置２７２、事前契約用メタデータ生成装置２７３を備える。

【００５７】顧客情報管理サーバ２６７とは、顧客情報生成システム２６６で生成された顧客情報の管理を行い、鍵管理サーバ２４５より個人鍵Km２６５、ユーザーが契約を行う事業者鍵Kw等の情報を受け取るためのユーザー情報１５０を生成し、鍵管理サーバ２４５に出力する。ユーザー情報１５０とは、例えば、ある端末IDの振られた受信側の受信端末に対し何人のユーザーが利用するか、また端末を利用するユーザーがどの放送事業者と契約を行うかを示した情報である。このユーザー情報１５０により鍵管理サーバー２４５は、管理する個人ID２７０/個人鍵Km２６５をユーザー情報に格納されているユーザー数分確保し、同じくユーザー情報に格納されている端末ID２４９に対応する端末鍵Kmc４３、各ユーザーが契約を行う事業者IDに対応する事業者鍵Kwを顧客情報管理サーバ２６７に受け渡すことが可能となる。顧客情報管理サーバ２６７は受け取った個人ID２７０、個人鍵Km２６５、端末ID２４９、端末鍵Kmc４３、事業者ID、事業者鍵Kwを顧客情報に追加することによりユーザーの使用する端末、ユーザー自身の個人情報、契約情報等の把握が可能となり顧客管理が可能となる。ICカード生成装置２７２は、顧客情報管理サーバ２６７内の顧客情報をもとに空ICカード内の所定エリアに個人ID２７０、個人鍵Kmc２６５、端末ID２４９、各ユーザーの名前、電話番号、生年月日等の個人契約情報を格納し各ユーザー１０６に配布する。事前契約用メタデータ生成装

置２７３とは、ICカード生成装置２７２と同様に顧客情報管理サーバ２６７内の顧客情報により各ユーザーの契約する事業者のID、事業者鍵Kw、契約形態を示す契約コードおよび、各ユーザーに割り振られた個人ID２７０、各ユーザーが使用する受信端末のID２４９を格納した事前契約用メタデータを生成し配信センタ内のメタデータ暗号化装置２２６に受け渡す。以上が送出側システムの構成及び、各装置間のデータフローである。

【００５８】（送出側で生成配信される情報）次に送出側で生成し、受信端末に対して配信される各メタデータについて説明する。本総合データ配信サービスにおけるメタデータの記述方式は、前述の図６におけるXML等のテキスト形式での記述、PSI/SIのようなバイナリ形式での記述が可能である。ただし、暗号化が必要な部分については受信端末内での記述内容解釈処理の向上の点で特にバイナリ形式での記述を行うが、受信端末の処理性能が高い場合は、非暗号化部分と同様にテキスト形式での記述による運用も可能である。各メタデータの記述内容、構成について説明する。

【００５９】（事前契約用メタデータ）図３０に、事前契約用メタデータの構成および格納される情報の説明図を示す。まず、事前契約用メタデータについて図３０を用いて説明する。事前契約用メタデータ２６３とは、前述の通り有料放送事業者の事業者鍵Kwや、契約形態に間する契約コード等の内容を含み、主に限定受信を行う際の判定材料に利用されるデータであり、端末購入時、契約更新時、事業者鍵Kwの更新時等に配信されるメタデータである。端末ID、個人ID等の受信端末が端末を利用するユーザー宛に送られたデータかを識別するためのユーザー識別情報２７５と、メタデータの暗号方式、暗号化部分、暗号鍵を示すID（端末ID）等のメタデータにかけられた暗号に関する暗号化情報２７６と、ユーザーの名前、電話番号、住所、決済能力、決済先、パスワード等のユーザー自身の個人情報２７７と、ユーザーが契約を行う契約事業者のID、事業者鍵Kw、契約の有効期限、契約コード、契約ポイント等の契約情報２７８等を含む。暗号化部分については、各ユーザーの決済先等の情報が格納される個人情報２７７、事業者鍵Kw等の情報が格納される契約情報２７８が該当し、ユーザーの利用する端末固有の鍵Kmc４３により送出側で暗号化され、受信端末に配信される。暗号化に使用する暗号鍵については運用により個人鍵Kmを使用することも可能である。また、運用により事前契約用メタデータに上記の情報以外に後述するメタデータ属性情報が格納されることも可能である。

【００６０】（EPG用メタデータ）図３１に、EPG用メタデータの構成および格納される情報の説明図を示す。次にEPG用メタデータ２５４について図３１を用いて説明する。EPG用メタデータ２５４とは、主にユーザーが配信予定コンテンツの確認、配信予定コンテンツの視聴/蓄積予約を行うためのメタデータであり、EPG用メタデータの配信時が蓄積/再生用メタデータ、鍵配信用メタデータの配信時と重なるため各メタデータを識別するためのメタデータID、メタデータのタイプ、メタデータのサイズ等のメタデータ属性情報２７９と、事前契約用メタデータと同様にメタデータの暗号部分に関する暗号化情報２７６と、番組のID、放送予定日時、番組の内容、ジャンル、コンテンツの構成、番組のサイズ等の番組に関する番組情報２８０と、コンテンツのID、コンテンツの内容、エレメントの構成等のコンテンツ情報２８１と、コンテンツを利用するユーザー、コンテンツ自体に対する制限情報である年齢制限、コピー制限、蓄積制限等の利用制限情報２８２等を含む。暗号化部分についてはコピー制限等の利用制限情報２８２が該当し、全ユーザーのメタデータの利用を可能とするため、全受信端末共通のシステム鍵Ksy２６４により送出側で暗号化され配信される。コンテンツ情報２８１については、総合データ配信サービスにおけるEPGの運用レベルにより格納せずに配信することも可能とする。利用制限情報についても同様に格納せずに運用を行う場合もあり、EPG用メタデータは暗号化せずに配信されることも可能である。

【００６１】（蓄積/再生用メタデータ）図３２に、蓄積/再生用メタデータの構成および格納される情報の説明図を示す。次に蓄積/再生用メタデータ２５５について図３２を用いて説明する。蓄積/再生用メタデータ２５５とは、コンテンツの受信、蓄積、再生に必要な情報を含むメタデータであり、蓄積済みコンテンツの検索時に利用される他、ユーザーのコンテンツ利用方法を制御するために利用される。蓄積/再生用メタデータは、EPG用メタデータと同様にメタデータ自体を識別するためのメタデータ属性情報２７９と、暗号化情報２７６と、番組情報２８０と、コンテンツ情報２８１と、利用制限情報２８２と、蓄積/再生用メタデータが示すコンテンツの暗号化方式、暗号鍵ID等のコンテンツ暗号化情報、コンテンツを視聴するための契約に関する、契約形態、契約による利用可能期間等の契約情報２８４と、契約による課金料金、課金タイミング等の課金情報２８５等を含む。暗号化部分については利用制限情報２８２、コンテンツの暗号化方式、暗号鍵ID等の情報が含まれるコンテンツ暗号化情報２８３、使用制限期間等の情報が含まれる契約情報２８４、課金時の料金、タイミング等が含まれる課金情報２８５が該当し、コンテンツを暗号化した鍵と同じコンテンツ鍵Kk３３により送出側で暗号化され配信される。また、蓄積/再生用メタデータにおけるコンテンツ情報２８１については、EPG用メタデータ内に格納されるコンテンツ情報にコンテンツの配信位置等の情報が追加される。

【００６２】（鍵配信用メタデータ）図３３に、鍵配信用メタデータの構成および格納される情報の説明図を示す。次に鍵配信用メタデータ２５６について図３３を用

いて説明する。鍵配信用メタデータ２５６とは、コンテンツの暗号鍵に関する情報を配信するためのメタデータであり、コンテンツが有料放送の場合は放送する事業者に契約したユーザーのみ受信可能とする限定受信を行うための情報が含まれる。鍵配信用メタデータ２５６は、他のメタデータより区別するためのメタデータ属性情報２７９と、メタデータ自体の暗号化に関する暗号化情報２７６と、コンテンツのID、コンテンツの暗号鍵Kk等のコンテンツ鍵情報２８６等を含む。暗号化部分に関してはコンテンツ鍵Kk等のコンテンツ鍵情報が送出側で暗号化され配信される。暗号鍵については、鍵配信用メタデータ２５６が有料コンテンツに対するメタデータであり、事業者に契約したユーザーのみ受信可能な限定受信を行う場合は、事業者毎に固有の事業者鍵Kw４４が使用され、契約者以外のユーザーも視聴可能な無料コンテンツに対するメタデータの場合は、全受信端末に共通なシステム鍵Ksy２６４が使用される。また、限定受信を実現させるための事業者ID、対象契約コード等の情報はコンテンツ鍵情報に格納され暗号化されて配信される。

【００６３】（メタデータリスト）図３４に、メタデータリストの構成および格納される情報の説明図を示す。次にメタデータリスト２５０について図３４を用いて説明する。メタデータリストとは、配信ストリーム中のEPG用メタデータ、蓄積/再生用メタデータ等の配信位置を取得するためのメタデータであり、PSIを補完する情報を持ち、受信端末内に蓄積したEPG用メタデータに対し配信ストリーム中のEPG用メタデータが更新された場合における差分メタデータ蓄積のための情報を含む。メタデータリスト２５０は、受信端末側で情報の更新を識別するためのバージョン等のメタデータリスト属性情報２８７と、コンテンツIDに対応するメタデータのID、EPG用メタデータ、蓄積/再生用メタデータを区別するためのメタデータタイプ、EPG用メタデータの更新を識別するためのメタデータのバージョン、配信ストリーム上の位置情報等のリスト情報２８８等を含む。メタデータリスト自体はメタデータを配信ストリームより取得するための情報であるため特に保護を必要とせず、暗号化は行わずに配信される。メタデータリストの取得方法としてはPSIテーブルにおけるPMT内に配信ストリームを指定することにより取得を行う運用とする。

【００６４】（システム鍵更新用メタデータ）図３５に、システム鍵更新用メタデータの構成および格納される情報の説明図を示す。次にシステム鍵更新用メタデータについて図３５を用いて説明する。システム鍵更新用メタデータ２８９とは、受信端末内に格納されている全受信端末共通の鍵であるシステム鍵Ksyをシステム鍵Ksy3に更新するためのメタデータである。システム鍵更新用メタデータ２８９は、他のメタデータと区別するためのメタデータ属性情報２７９と、メタデータ自体の暗号化に関する暗号化情報２７６と、更新対象となるシステム鍵に対応するシステムID、変更後のシステムID、システム鍵、更新タイミング等の情報が含まれるシステム鍵情報２９０等を含む。

【００６５】暗号化部分は、更新後のシステム鍵、変更タイミング等の情報が含まれるシステム鍵情報２９０が該当し、暗号鍵は受信端末内に予め予備用のシステム鍵として登録されているシステム鍵Ksy2を使用する。システム鍵Ksyは、システム鍵全体の総称で、通常は１つが有効である。ただし、ハック等の被害があった時に、予備のシステム鍵Ksy2を使用する。そのために、受信機には通常２つのシステム鍵Ksy1、Ksy2が内蔵されている。システム鍵Ksyの更新処理を具体的に説明するために、システム鍵Keyの実際の受信機内の構成である２つシステム鍵Key1、Key2について述べる。Key1、Key2が受信機内部に内蔵されており、これらの鍵を更新等の変更をする時に、システム鍵送信側は、他のシステム鍵Key3を衛星より伝送し、受信端末では、システム鍵Ksy1がKey3に変更となる。これより実際の受信機内には、システム鍵Key2、Ksy3の２つの鍵が存在することになる。また、システム鍵Key2が実際には有効鍵となる。以上が本総合データ配信サービスにおける送出側より配信されるメタデータである。

【００６６】５．受信側システム

つぎに、上述のサービスフローを実施させる受信側システムである受信端末について説明する。

（受信端末構成）図３６に、受信端末内の構成図を示す。次に本総合データ配信サービスにおける受信側である受信端末３について図３６を用いて説明する。受信端末３は衛星を介したコンテンツ１７、PSI/SI１９、メタデータ１８等の情報をアンテナ２により受信し、TV９等のモニタ装置に出力、また蓄積媒体４内に蓄積後出力することでユーザーの視聴を可能とする。将来的にはこの受信端末３がTV９等のモニタ装置に内蔵されることもあるがここでは一例として、別装置として説明する。総合データ配信サービス用の受信端末３の大きな特徴としては、コンテンツ１７及びメタデータ１８等の情報を蓄積するための蓄積媒体４を有している他に、暗号化し配信されたデータの復号及び受信端末内で生成される重要なデータに対し暗号化を行い、著作権保護等の権利、認証、課金等の処理、制御に関わるRMP１６機能、この受信端末を利用するユーザーの個人認証、及びユーザーの属する家族等のグループ認証を行う個人認証デバイスであるICカード１５を有していることである。このRMP１６機能とは、メタデータの内容を解釈し権利保護に関わる処理の制御を行うRMPコントローラ３０６、暗号化されたメタデータを復号するメタデータ復号機能３０７、暗号化されたコンテンツを復号するためのコンテンツ復号機能３０８、受信端末内で使用する鍵を管理する鍵管理テーブル３１１、受信端末を利用するユーザーの環境を設定するためのプロファイル３１０、受信端末内でメ

タデータ等より生成されるコンテンツの視聴を許諾する情報等の保護が必要なデータを暗号化するメタデータ暗号機能３０９等を含む。蓄積媒体４は、前述のコンテンツ１７、メタデータ１８の他に、受信端末内で生成される予約情報３１３、検索/EPGテーブル３１２等の情報が格納される受信端末に固定的な大容量蓄積媒体であるハードディスクや、必要なコンテンツ、メタデータ等の情報を格納する取り外し可能なDVD-RAM、メモリカード等のリムーバブルメディアを備える。ICカード１５は、前述した個人ID２７０、個人鍵２６５、個人契約情報２７４の他に、受信端末内で生成されるコンテンツの視聴を許諾する判断材料となる許諾情報３１４等が格納される。RMP１６については、パイレーツや暗号解読などに対するセキュリティ対策としセキュリティの守られた構成よりなるが、セキュリティ強度の退化等によりモジュールごと取り替えることが可能な構成も考えられる。

【００６７】次に受信端末の特徴的な機能であるRMP１６、蓄積媒体４、ICカード１５について説明する。

（RMP）本総合データ配信サービスにおけるRMP１６機能とは、メタデータの内容を解釈し権利保護に関わる処理の制御を行うRMPコントローラ３０６、暗号化されたメタデータを復号するメタデータ復号機能３０７、暗号化されたコンテンツを復号するためのコンテンツ復号機能３０８、受信端末内で使用する鍵を管理する鍵管理テーブル３１１、受信端末を利用するユーザーの環境を設定するためのプロファイル３１０、受信端末内でメタデータ等より生成されるコンテンツの視聴を許諾する情報等の保護が必要なデータを暗号化するメタデータ暗号機能３０９等を含む。

【００６８】図５２に、RMPコントローラ３０６の行う主な制御処理について示す。RMPコントローラ３０６の主な機能としては、図示のように、例えば、受信制御、蓄積制御、コピー制御、提示制御、視聴契約制御、課金制御、個人認証制御、鍵管理、プロファイル管理、時刻管理、アプリケーション認証制御、外部機器認証制御、外部機器認証制御、通信回線制御がある。

【００６９】（メタデータ復号）図３７に、メタデータ復号機能の説明図を示す。次にメタデータ復号について図３７を用いて説明する。メタデータ復号機能３０７とは、RMPコントローラ３０６より復号要求が起こった際に、鍵管理テーブル３１１よりRMPコントローラ３０６を介して受け渡される暗号鍵を使用し、暗号化されたメタデータ等を復号する機能である。RMPコントローラ３０６は、コンテンツの受信/蓄積時、コンテンツの視聴契約時等でメタデータを復号する必要があると判断した場合、まず蓄積媒体内の暗号化されたメタデータもしくはICカード内の暗号化された個人契約情報等を複製し、各データの非暗号化部分に格納されている前述した暗号化情報内の暗号鍵IDを読み取り、暗号鍵IDを鍵管理テーブル３１１に受け渡す。鍵管理テーブル３１１は受け渡された暗号鍵IDより対応する暗号鍵を識別し、RMPコントローラ３０６に対し暗号鍵を受け渡す。RMPコントローラ３０６は、鍵管理テーブルより受け渡された暗号鍵と、メタデータをメタデータ復号機能３０７に受け渡し、復号を要求する。メタデータ復号機能３０７は、受け渡されたメタデータの暗号部分を抽出し、抽出した暗号部分をRMPコントローラ３０６より同じく受け渡された暗号鍵により復号し、非暗号化部分のメタデータの所定部分に格納し、RMPコントローラ３０６に復号したメタデータとして受け渡す。ただし、復号したデータについては前述した通り運用により非暗号化部分とデータ形式が異なる場合があるため、その際は格納せずにその後の処理を行う運用を行うこともある。以上がメタデータ復号機能３０７の復号処理である。メタデータ復号機能３０７が復号するメタデータとは、EPG用メタデータ２５４、蓄積/再生用メタデータ２５５、鍵配信用メタデータ（無料）２６１、鍵配信用メタデータ（有料）２６２、事前契約用メタデータ２６３、システム鍵更新用メタデータ２８９の各メタデータの他に、ICカードに格納される個人契約情報２７４、許諾情報３１４が挙げられる。ICカード内の情報である個人契約情報２７４、許諾情報３１４については、暗号鍵が鍵テーブルに格納されていないため、ICカード内の個人鍵Km２６５をRMPコントローラ３０６より取得し復号を行う。

【００７０】（コンテンツ復号）図３８に、コンテンツ復号機能の説明図を示す。コンテンツ復号について図３８を用いて説明する。コンテンツ復号機能３０８とは、RMPコントローラ３０６の復号要求に対し、鍵管理テーブル３１１よりRMPコントローラ３０６を介し受け取ったコンテンツの暗号鍵であるコンテンツ鍵を使用し、コンテンツ１７内の各エレメントを復号する機能であり、主にコンテンツの再生時に行われる処理である。

【００７１】（プロファイル）図３９に、プロファイルの構成図を示す。次にプロファイルについて図３９を用いて説明する。プロファイル３１０とは、事前契約用メタデータ２６３よりRMP内で生成される個人契約情報２７４の集合であり、保護の必要なデータであるため、RMP内部のセキュリティの守られた記憶エリア（セキュアメモリ）３１７に格納され、コンテンツの視聴/蓄積予約、限定受信の判定時等に使用される。プロファイル３１０は端末ユーザー全体に対する契約情報等の格納された全体プロファイル３１５と、各ユーザー毎の契約情報が格納された個人プロファイル３１６を含む。

【００７２】（鍵管理テーブル）図４０に、鍵管理テーブルの構成図を示す。鍵管理テーブルについて図４０を用いて説明する。鍵管理テーブル３１１とは、RMPコントローラ３０６より指定されるIDに対して該当する鍵を受け渡すための情報であるID及び鍵を格納したテーブルであり、保護の必要な鍵データより構成されるため、プロファイルと同様にRMP内部のセキュリティの守られた

記憶エリア（セキュアメモリ）３１７に格納される。

【００７３】（メタデータ暗号）図４１に、メタデータ暗号機能の説明図を示す。メタデータ暗号について図４１を用いて説明する。メタデータ暗号機能３０９とは、RMP１６よりICカード１５に対し事前契約用メタデータより生成した個人契約情報２７４や、蓄積/再生用メタデータより生成したコンテンツの許諾情報３１４を格納する際に、各情報をICカード１５内の個人鍵Km２６５を用いて暗号化する機能である。

【００７４】（蓄積媒体）図４２に、蓄積媒体内に格納される情報の蓄積状態の説明図を示す。次に受信端末３における蓄積媒体４に格納されるデータの蓄積状態について図４２を用いて説明する。蓄積媒体４に格納されるデータとしては、メタデータリスト２５０、EPG用メタデータ２５４、検索/EPGテーブル３１２、予約情報３１３、蓄積/再生用メタデータ２５５、コンテンツ１７、その他受信端末のOS、アプリケーション等のソフトウェア等が存在する。蓄積媒体４自体は、この例では、セキュリティの保護された構造ではないため、蓄積媒体内に格納されるデータにおいて保護の必要なデータは、暗号化状態で蓄積される。EPG用メタデータ２５４や蓄積/再生用メタデータ２５５等を受信するためのメタデータリスト２５０と、EPG用メタデータ２５４や蓄積/再生用メタデータ２５５より生成され、受信端末のEPG表示、検索処理を行うための検索/EPGテーブル３１２と、EPG用メタデータ２５４より生成されるコンテンツ視聴/蓄積予約のための予約情報３１３とは特に保護の必要とされないデータであるため暗号化せずに蓄積媒体に格納される。ただし運用において保護が必要な場合は、端末内に予め存在する端末鍵Kmc等により暗号化を行う。コンテンツの利用制限情報等が格納されたEPG用メタデータ２５４、蓄積/再生用メタデータ２５５、コンテンツ１７については送出側で暗号化された状態で蓄積され、各データが処理に必要な際はコピーを生成し、コピーを復号し利用することにより受信端末内での再暗号化処理を省くことが可能となる。

【００７５】（ICカード）図４３に、ICカード内の構成の説明図を示す。総合データ配信サービスにおいて利用されるICカード１５内の構成について図４３を用いて説明する。ICカード１５内は、セキュリティの守られた記憶エリア（セキュアメモリ）３１７と通常の記憶エリア（通常メモリ）３１８を備える。通常の記憶エリア３１８では、保護の必要でないデータもしくは、保護が必要であるが暗号化することで保護されているデータが格納され、一方、セキュリティの守られた記憶エリア３１７に格納される情報は保護が必要なデータであるがICカード内で暗号化状態で保存できない情報が格納される。セキュリティが守られた記憶エリア３１７に格納される情報としては、ユーザー個人に割り当てられた個人ID２７０、それに対応する暗号鍵である個人鍵Km２６５等が該当し、一方、通常の記憶エリア３１８に格納されるデータは、RMP１６側で暗号化された個人契約情報２７４、許諾情報３１４等が該当する。また、セキュリティの守られた記憶エリア３１７に格納された個人ID２７０、個人鍵２６５をRMP１６に受け渡す場合は、同じくセキュリティの守られた伝送路を使用し、データの受け渡しを行う。セキュリティの守られた伝送路とは、公開鍵方式等を利用することにより実現する。

【００７６】（受信端末側で生成される情報）次に総合データ配信サービスにおいて受信端末内で生成される各情報の生成時の処理について説明する。

【００７７】（プロファイル生成）図４４に、プロファイルの生成処理の説明図を示す。まず事前契約用メタデータより生成されるプロファイルについて図４４を用いて説明する。プロファイル３１０とは、事前契約用メタデータ２６２を元にRMP内部で生成される情報である。プロファイル３１０の生成は、まず、送出側より受信した事前契約用メタデータ２６３をメタデータ復号機能により復号したのち、RMPコントローラ３０６により、事前契約用メタデータ２６３のユーザー識別情報２７５内の端末ID、個人IDにより端末全体用の契約情報か、各ユーザー用の契約情報かを判定し、メタデータ復号機能により復号された個人情報２７７、契約情報２７８より必要な情報のみを抽出し個人契約情報２７４を生成する。さらに、その個人契約情報２７４を、ユーザー識別情報２７５により識別したセキュリティエリア３１７内の全体プロファイル３１５、個人プロファイル３１６の各プロファイルに格納することにより、プロファイル３１０が生成される。

【００７８】（鍵管理テーブル）図４５に、鍵管理テーブルの生成処理の説明図を示す。次に鍵管理テーブルの生成時の処理について図４５を用いて説明する。鍵管理テーブル３１１には、ユーザーの受信端末購入時に予め格納されているID、鍵情報と、ユーザーがサービス受信時に生成されるID、鍵情報が存在する。予め格納されている情報としては、端末ID２４９、端末鍵Kmc４３、システムID２４７、システム鍵Ksy２６４が存在する。なお、システム鍵Ksyは、システム鍵Ksy1～Ksy3等のシステム鍵の総称である。この例では、システムID、鍵については、運用に使用されるID、鍵情報Ksy1と、システム鍵更新時に利用される予備用のID、鍵情報Ksy2の２種類が存在する。受信側で生成もしくは更新される部分としては、システム鍵更新時のシステムID２４７、システム鍵Ksy２６４、事業者ID２４８、事業者鍵Kw４４、コンテンツID２４６、コンテンツ鍵Kk３３が該当する。生成される各ID、鍵情報は、受信端末が受信したシステム鍵更新用メタデータ２８９、事前契約用メタデータ２６３、鍵配信用メタデータ２５６内の暗号化部分に格納されているため、RMP１６内部のメタデータ復号により復号後に、RMPコントローラにより各メタデータから抽出

され、セキュリティの守られた記憶エリア３１７に格納することにより鍵管理テーブル３１１を生成する。

【００７９】（検索/EPGテーブル）図４６に、検索/EPGテーブルの生成処理の説明図を示す。検索/EPGテーブルについて図４６を用いて説明する。検索/EPGテーブル３１２とは、受信したEPG用メタデータ２５４、蓄積/再生用メタデータ２５５よりRMP内部にコピーを作成し、メタデータ復号機能により各メタデータを復号後に、RMPコントローラにより必要項目を抽出し、蓄積媒体４内の所定位置に格納することにより生成される。検索/EPGテーブル３１２は、蓄積媒体内に複数存在するEPG用メタデータ２５４、蓄積/再生用メタデータ２５５の簡易情報の集合である。また、検索/EPGテーブル３１２は、暗号化せずに蓄積媒体に格納される情報であるため、受信端末上の検索アプリケーション、EPGアプリケーションから直接アクセス可能となり、受信端末の検索スピード、EPG表示スピードの向上が可能となる。

【００８０】（予約情報）図４７に、予約情報の生成処理の説明図を示す。次に予約情報について図４７を用いて説明する。予約情報３１３とは、ユーザーの視聴/蓄積要求に対しRMP１６内部でEPG用メタデータ２５４、プロファイル３１０より生成される情報であり、暗号化せずに蓄積媒体４に格納される情報である。ユーザーより視聴/蓄積要求が起こると、RMPコントローラ３０６は、視聴要求の対象となるコンテンツに対するEPG用メタデータ２５４のコピーをRMP内部に生成し、コピーしたEPG用メタデータをメタデータ復号機能により復号する。そして、RMPコントローラ３０６は、復号したEPG用メタデータの利用制限情報と、プロファイル内の予約要求を行ったユーザーの個人契約情報とにより、コンテンツ自体の予約が可能か、ユーザーの契約形態が要求コンテンツの予約が可能かを判定し、その後蓄積媒体４内の他の予約情報３１３により登録済みの予約がないか、スケジュール的に予約が可能か等を判定する。ここで、RMPコントローラ３０６は、予約が可能であれば個人契約情報より予約を行ったユーザーの個人ID、EPG用メタデータ２５４より、コンテンツID、コンテンツサイズ、放送予定日時等、ユーザーの要求より予約の種別を抽出し予約情報３１３を生成し、蓄積媒体４内の所定位置に格納することで予約を行う。ユーザーの嗜好性を利用した自動蓄積を行わせる場合も同様に予約情報を生成する。

【００８１】（ICカード内の個人契約情報）図４８に、個人契約情報の生成処理の説明図を示す。次にプロファイル内の個人契約情報をICカードに格納する際の暗号化処理について図４８を用いて説明する。ICカード１５内の個人契約情報とは、基本的にRMP１６内のセキュリティの守られた記憶エリア上のプロファイル内に格納されている個人契約情報２７４を暗号化させたものである。RMPコントローラ３０６は、ICカード１５が挿入されたことを認識するとICカード１５内のセキュリティエリア上の個人ID２７０をセキュリティの守られた伝送路を通じて読み取り、プロファイル内の該当個人契約情報を識別する。次に、RMPコントローラ３０６は、ICカード１５内に個人契約情報が存在すれば、それを読み取りメタデータ復号機能によりそれを復号し、互いの個人契約情報の非暗号化部分に格納されるバージョンNo.を確認し、ICカードのバージョンが新しい場合は、ICカード側の暗号化された個人契約情報をRMP内にコピーし、ICカード１５よりセキュリティの守られた伝送路を通じて取得した個人鍵Km２６５を使用しメタデータ復号により個人契約情報を復号し該当するプロファイル内の個人契約情報を更新する。RMPコントローラ３０６は、逆にプロファイル側の個人契約情報２７４のバージョンが新しい場合は、ICカード１５よりセキュリティの守られた伝送路を通じて取得した個人鍵Km２６５を使用し、メタデータ暗号機能３０９により個人契約情報の必要部分を暗号化したのちICカード１５内の所定の位置に格納することにより個人契約情報の更新を行う。

【００８２】（許諾情報）図４９に、許諾情報の生成処理の説明図を示す。次に許諾情報について図４９を用いて説明する。許諾情報３１４とは、コンテンツの視聴に対しての権利情報であり、RMP１６内でICカード１５内の個人契約情報２７４と、蓄積媒体４内の蓄積/再生用メタデータ２５５のコピーより生成される。ユーザーのコンテンツに対する視聴要求が起こると、RMPコントローラ３０６は該当するコンテンツに対する蓄積/再生用メタデータ２５５のコピーをRPM１６内部に生成し、コピーした蓄積/再生用メタデータ２５５をメタデータ復号機能により復号する。蓄積/再生用メタデータを復号化した後、RMPコントローラ３０６は、ICカード１５内より暗号化された個人契約情報２７４及び、セキュリティの守られた伝送路を通じて個人鍵Km２６５を取得し、メタデータ復号により個人契約情報２７４を復号する。個人契約情報を復号化した後、RMPコントローラ３０６は、蓄積/再生用メタデータ２５５内の利用制限情報と、個人契約情報によりユーザーが視聴可能なコンテンツかを判定し、ユーザーの選択する視聴契約形態により、蓄積/再生用メタデータ内の契約情報、課金情報等より必要な項目を抽出し許諾情報３１４を生成し、ICカード１５より取得した個人鍵Kmを使用しメタデータ暗号機能３０９により暗号化したのちICカード内の所定位置に暗号化された許諾情報を格納する。また受信端末内でユーザーの嗜好性による自動蓄積予約、画面表示の変化などの処理を行わせる場合は、許諾情報内のジャンル等の情報を集計することによりユーザーの嗜好性を判断することで、処理が可能となる。以上が総合データ配信サービスにおける受信端末内で生成される情報に対する処理である。総合データ配信サービスは、前述の送出側より配信される各メタデータ、受信側である受信端末内で配信されたメタデータを利用し各情報を生成、使用する

ことによりコンテンツの著作権、その他放送事業者、ユーザー等の権利保護を可能とする。

【００８３】

【発明の効果】本発明によると、以上のように、蓄積型放送かつ、コンテンツの保護が可能となる制御情報を付加するデータ配信サービス方法を提供することができる。

【図面の簡単な説明】

【図１】総合データ配信サービスの受信側の構成図。

【図２】総合データ配信サービスの全体システム構成図。

【図３】総合データ配信サービスにおける権利保護方式の説明図。

【図４】総合データ配信サービスと既存サービスの暗号化方式比較の説明図。

【図５】コンテンツの暗号化方式の説明図。

【図６】メタデータの暗号化方式の説明図。

【図７】総合データ配信サービスにおける限定受信方式の説明図。

【図８】事前契約による課金方式の説明図。

【図９】上り回線を必要としない視聴契約に対する課金方式の説明図。

【図１０】上り回線を使用したオンライン課金方式の説明図。

【図１１】総合データ配信サービスにおけるサービスの流れの説明図。

【図１２】事前契約におけるサービスフローの説明図。

【図１３】送出側におけるサービスフローの説明図。

【図１４】受信側におけるサービスフローの説明図。

【図１５】送出側システム全体の構成図。

【図１６】配信センタ内の構成図。

【図１７】オーサリングシステム内の構成図。

【図１８】番組構成管理システム内の構成図。

【図１９】PSI/SI生成装置の説明図。

【図２０】メタデータ生成装置の説明図。

【図２１】コンテンツ暗号化装置の説明図。

【図２２】メタデータ暗号化装置の説明図。

【図２３】送出系システム内の構成図。

【図２４】鍵管理センタ内の構成図。

【図２５】鍵生成装置の説明図。

【図２６】鍵管理サーバの説明図。

【図２７】顧客管理センタ内の構成図。

【図２８】顧客情報生成システム内の構成図。

【図２９】顧客情報管理システム内の構成図。

【図３０】事前契約用メタデータの構成および格納される情報の説明図。

【図３１】EPG用メタデータの構成および格納される情報の説明図。

【図３２】蓄積/再生用メタデータの構成および格納される情報の説明図。

【図３３】鍵配信用メタデータの構成および格納される情報の説明図。

【図３４】メタデータリストの構成および格納される情報の説明図。

【図３５】システム鍵更新用メタデータの構成および格納される情報の説明図。

【図３６】受信端末内の構成図。

【図３７】メタデータ復号機能の説明図。

【図３８】コンテンツ復号機能の説明図。

【図３９】プロファイルの構成図。

【図４０】鍵管理テーブルの構成図。

【図４１】メタデータ暗号機能の説明図。

【図４２】蓄積媒体内に格納される情報の蓄積状態の説明図。

【図４３】ICカード内の構成の説明図。

【図４４】プロファイルの生成処理の説明図。

【図４５】鍵管理テーブルの生成処理の説明図。

【図４６】検索/EPGテーブルの生成処理の説明図。

【図４７】予約情報の生成処理の説明図。

【図４８】個人契約情報の生成処理の説明図。

【図４９】許諾情報の生成処理の説明図。

【図５０】映像系及びデータ系コンテンツを構成するデータの説明図。

【図５１】本総合データ配信サービスにおいてコンテンツ、前述した各メタデータを暗号化する際に使用する暗号鍵、暗号鍵についての説明図。

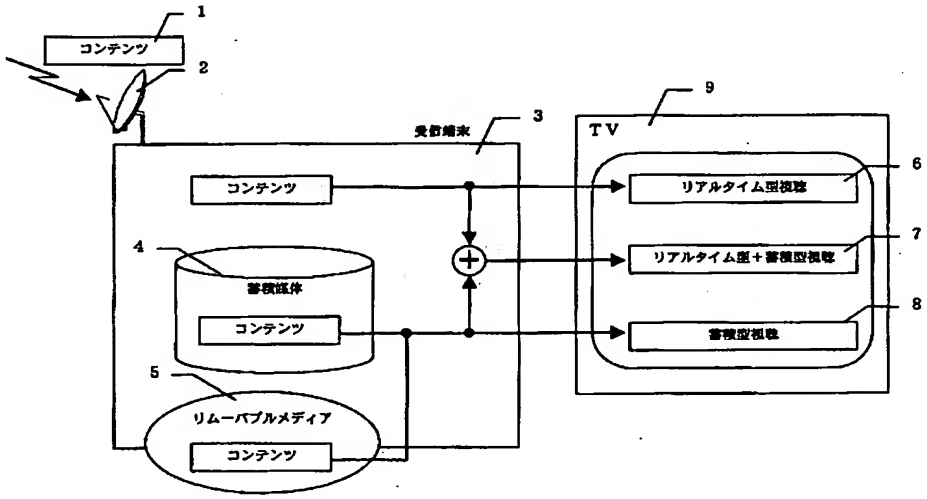
【図５２】RMPコントローラ３０６の行う主な制御処理の説明図。

【符号の説明】

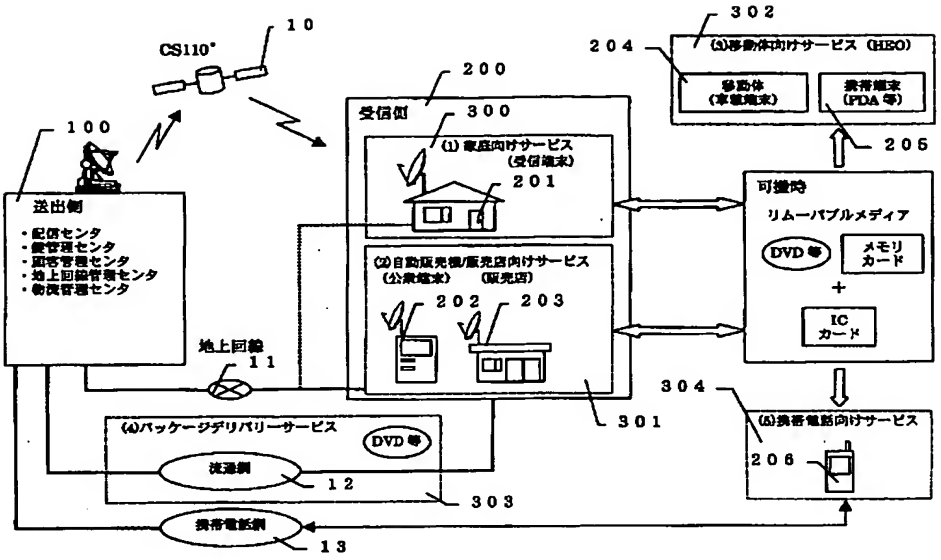
１…コンテンツ、２…アンテナ、３…受信端末、４…蓄積媒体、５…リムーバブルメディア、６…リアルタイム型視聴、７…リアルタイム型＋蓄積型視聴、８…蓄積型視聴、９…TV、１０…衛星、１１…地上回線、１２…流通網、１３…携帯電話網、１４…外部機器、１５…ICカード、１６…RMP、１７…暗号化コンテンツ、１８…暗号化メタデータ、１９…PSI/SI、２０…コンテンツ生成、２１…TSP化、２２…ペイロード、２３…コンテンツの一部、２４…ペイロード部分の暗号化、２５…コンテンツ暗号化、２６…暗号化コンテンツの一部、２７…映像系コンテンツ、２８…データ系コンテンツ、２９…MPEG2-Video (PES)、３０…MPEG2-AAC (PES)、３１…暗号化MPEG2-Video (PES)、３２…暗号化MPEG2-AAC (PES)、３３…Kk1、３４…Kk2、３５…暗号化必要部分、３６…暗号化データ容量、３７…暗号化データ、３８…非暗号化メタデータ、３９…契約要求、４０…事前契約用メタデータ、４１…鍵配信用メタデータ、４２…蓄積/再生用メタデータ、４３…端末鍵Kmc、４４…事業者鍵Kw、４５…ユーザー毎に配信、４６…コンテンツ要求、４７…ユーザー登録、４８…指定口座、４９…ポイント要求、５０…課金情報、５１…PPV登録、１００…送出

側、１０１…送出側フロー、１０２…コンテンツ生成、１０３…メタデータ生成、１０４…暗号化/配信、１０５…事前契約フロー、１０６…ユーザー、１０７…顧客管理、１５０…ユーザー情報、２００…受信側、２０１…家庭、２０２…自動販売機、２０３…販売店、２０４…車載端末、２０５…携帯端末、２０６…携帯電話、２０８…番組編成、２０９…コンテンツ暗号化、２１０…PSI/SI生成、２１１…メタデータ暗号化、２１２…配信フォーマット化、２１３…物流管理センタ、２１４…地上回線管理センタ、２２０…配信センタ、２２１…オーサリングシステム、２２２…番組構成管理システム、２２３…メタデータ生成装置、２２４…PSI/SI生成装置、２２５…コンテンツ暗号化装置、２２６…メタデータ暗号化装置、２２７…送出系システム、２２８…映像オーサリングシステム、２２９…音声オーサリングツール、２３０…データオーサリングツール、２３１…コンテンツ構成装置、２３２…コンテンツ管理サーバ、２３３…関連ファイル、２３４…素材、２３５…番組構成装置、２３６…番組運行スケジュール生成装置、２３７…番組管理サーバ、２３８…運行スケジュール、２３９…カルーセル生成装置、２４０…鍵管理センタ、２４１…パケタイザ、２４２…MUX、２４３…受託放送設備、２４４…鍵生成装置、２４５…鍵管理サーバ、２４６…コンテンツID、２４７…システムID、２４８…事業者ID、２４９…端末ID、２５０…メタデータリスト、２５１…EPG用メタデータ、２５２…蓄積/再生用メタデータ、２５３…鍵配信用メタデータ、２５４…暗号化EPG用メタデータ、２５５…暗号化蓄積/再生用メタデータ、２５６…暗号化鍵配信用メタデータ、２５７…鍵配信用メタデータ（無料）、２５８…鍵配信用メタデータ（有料）、２５９…事前契約用メタデータ、２６０…顧客管理センタ、２６１…暗号化鍵配信用メタデータ（無料）、２６２…暗号化鍵配信用メタデータ（有料）、２６３…暗号化事前契約用メタデータ、２６４…システム鍵Ksy、２６５…個人鍵Km、２６６…顧客情報生成システム、２６７…顧客情報管理サーバ、２６８…ユーザーI/F、２６９…顧客情報生成装置、２７０…個人ID、２７１…顧客情報管理システム、２７２…ICカード生成装置、２７３…事前契約用メタデータ生成装置、２７４…個人契約情報、２７５…ユーザー識別情報、２７６…暗号化情報、２７７…個人情報、２７８…契約情報、２７９…メタデータ属性情報、２８０…番組情報、２８１…コンテンツ情報、２８２…利用制限情報、２８３…コンテンツ暗号化情報、２８４…契約情報、２８５…課金情報、２８６…コンテンツ鍵情報、２８７…メタデータリスト属性情報、２８８…リスト情報、２８９…システム鍵更新用メタデータ、２９０…システム鍵情報、３００…家庭向けサービス、３０１…自動販売機/販売店向けサービス、３０２…移動体向けサービス、３０３…パッケージデリバリサービス、３０４…携帯電話向けサービス、３０６…RMPコントローラ、３０７…メタデータ復号、３０８…コンテンツ復号、３０９…メタデータ暗号、３１０…プロファイル、３１１…鍵管理テーブル、３１２…検索/EPGテーブル、３１３…予約情報、３１４…許諾情報、３１５…全体プロファイル、３１６…個人プロファイル、３１７…セキュアメモリ、３１８…通常メモリ、３３１…受信側フロー、３３２…予約、３３３…コンテンツ受信/蓄積、３３４…視聴契約、３３５…再生

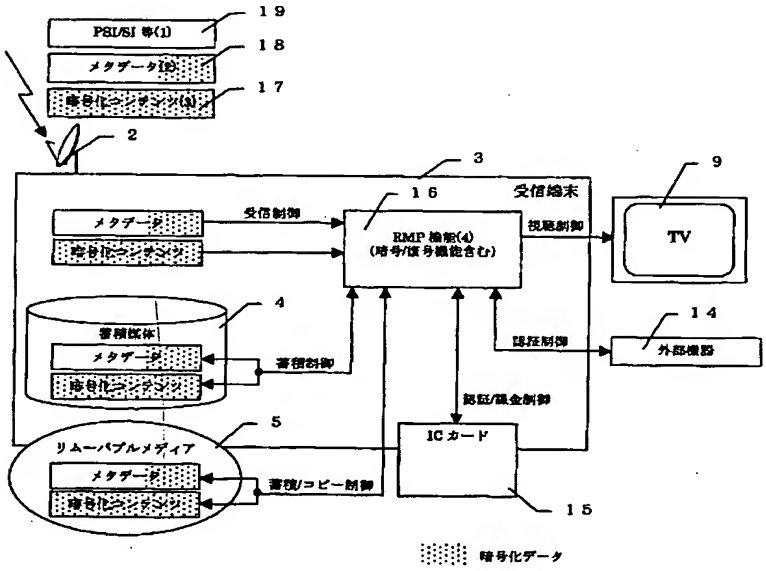
【図１】



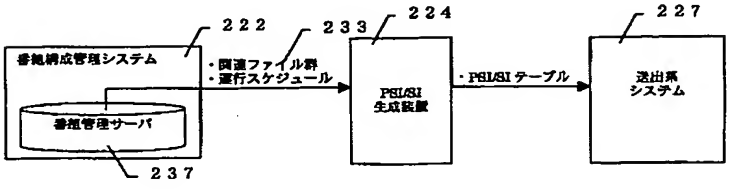
【図２】


CS110°
10
100
送出側
・配信センタ
・鍵管理センタ
・加入者管理センタ
・地上回線管理センタ
・動画管理センタ
地上回線
11
200
受信側
300
(1)家庭向けサービス
(受信端末)
201
(2)自動販売機/販売店向けサービス
(公衆端末)　(販売店)
202
203
301
(4)パッケージデリバリーサービス
DVD等
流通網
12
303
携帯電話網
13
302
(3)移動体向けサービス (HEO)
204
移動体
(車載端末)
携帯端末
(PDA等)
205
可搬時
リムーバブルメディア
DVD等
メモリカード
+
ICカード
304
(5)携帯電話向けサービス
206

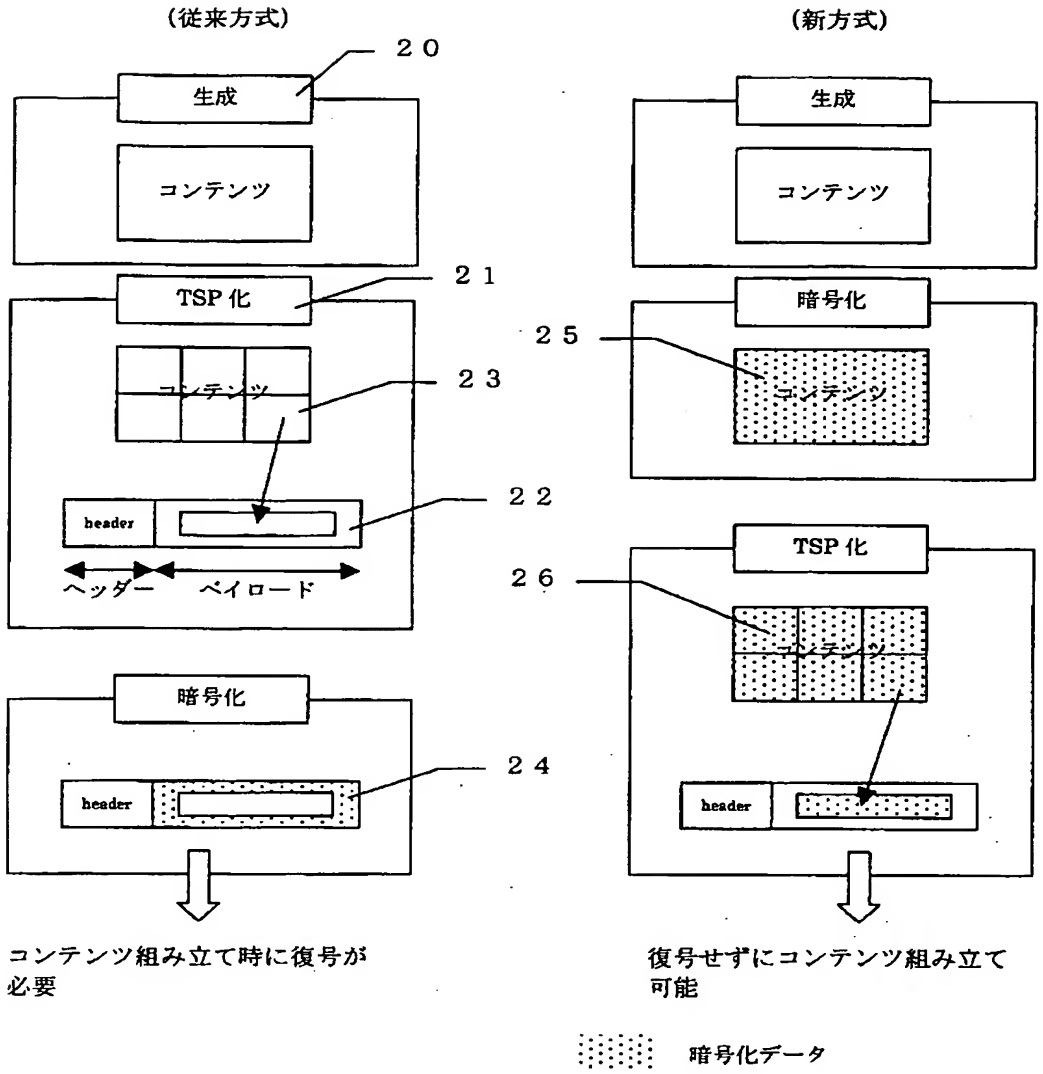
【図３】


19
PSI/SI等(1)
18
メタデータ(2)
17
暗号化コンテンツ(3)
2
3
受信端末
16
メタデータ
暗号化コンテンツ
受信制御
RMP機能(4)
(暗号/復号機能含む)
視聴制御
9
TV
4
蓄積媒体
メタデータ
暗号化コンテンツ
蓄積制御
課金制御
14
外部機器
認証/課金制御
5
リムーバブルメディア
メタデータ
暗号化コンテンツ
蓄積/コピー制御
ICカード
15
暗号化データ

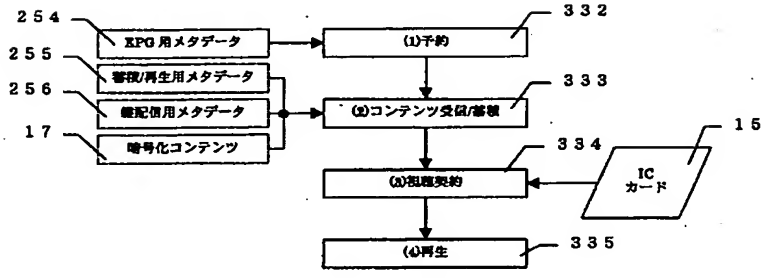
【図１９】


222
番組構成管理システム
番組管理サーバ
237
・関連ファイル群
・運行スケジュール
233
224
PSI/SI
生成装置
・PSI/SIテーブル
227
送出系
システム

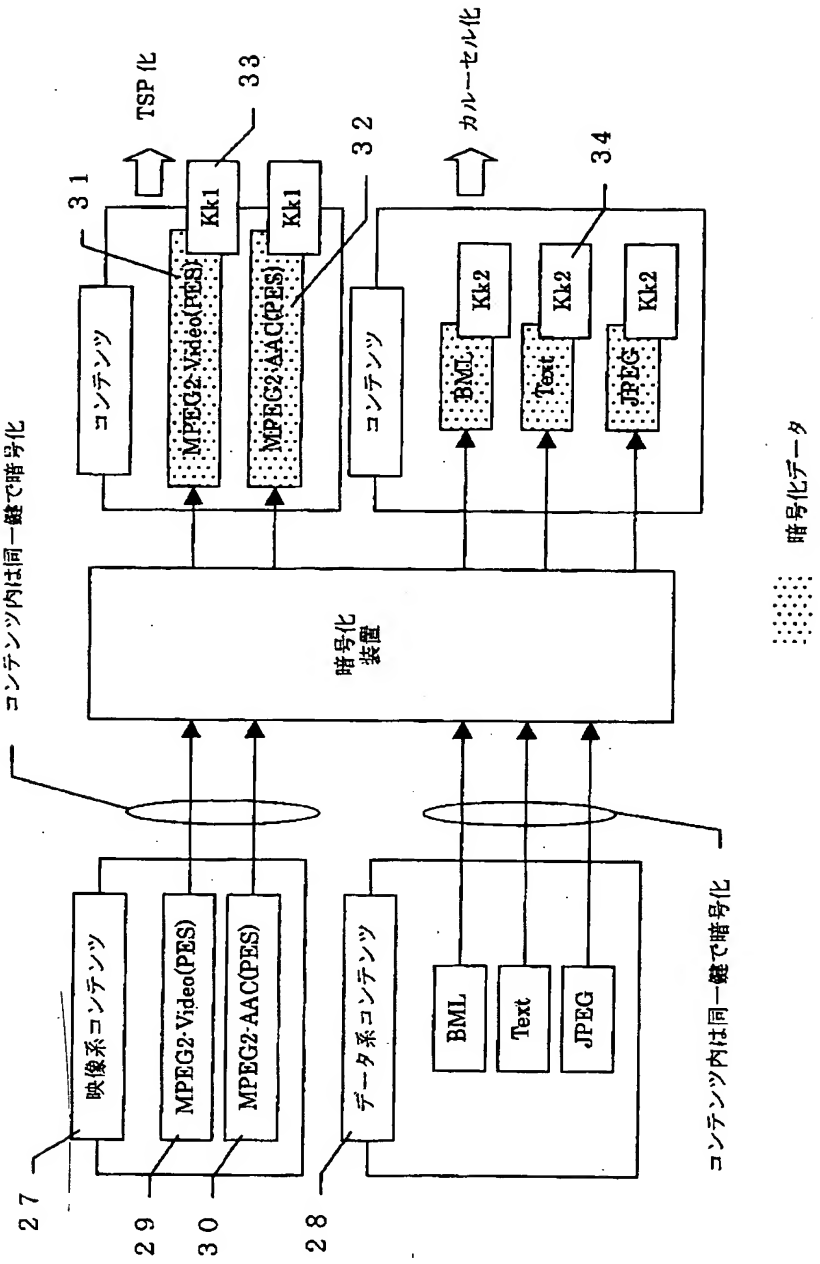
【図４】


(従来方式)
(新方式)
２０
生成
コンテンツ
２１
TSP 化
２３
２２
header
ヘッダー
ペイロード
暗号化
２４
２５
２６
コンテンツ組み立て時に復号が必要
復号せずにコンテンツ組み立て可能
暗号化データ

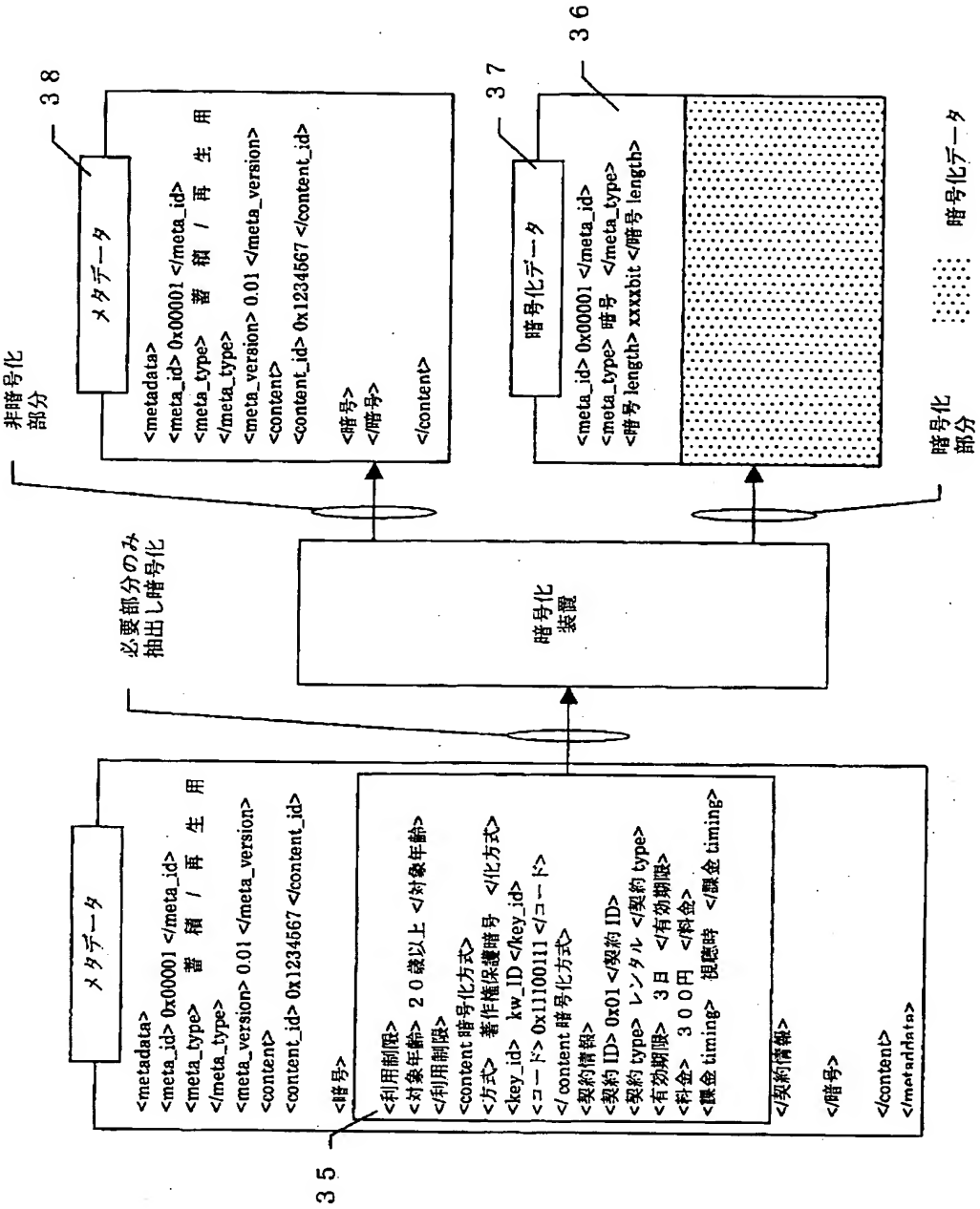
【図１４】


２５４
EPG 用メタデータ
２５５
蓄積/再生用メタデータ
２５６
課記信用メタデータ
１７
暗号化コンテンツ
(1)予約
３３２
(2)コンテンツ受信/蓄積
３３３
(3)視聴契約
３３４
１５
IC カード
(4)再生
３３５

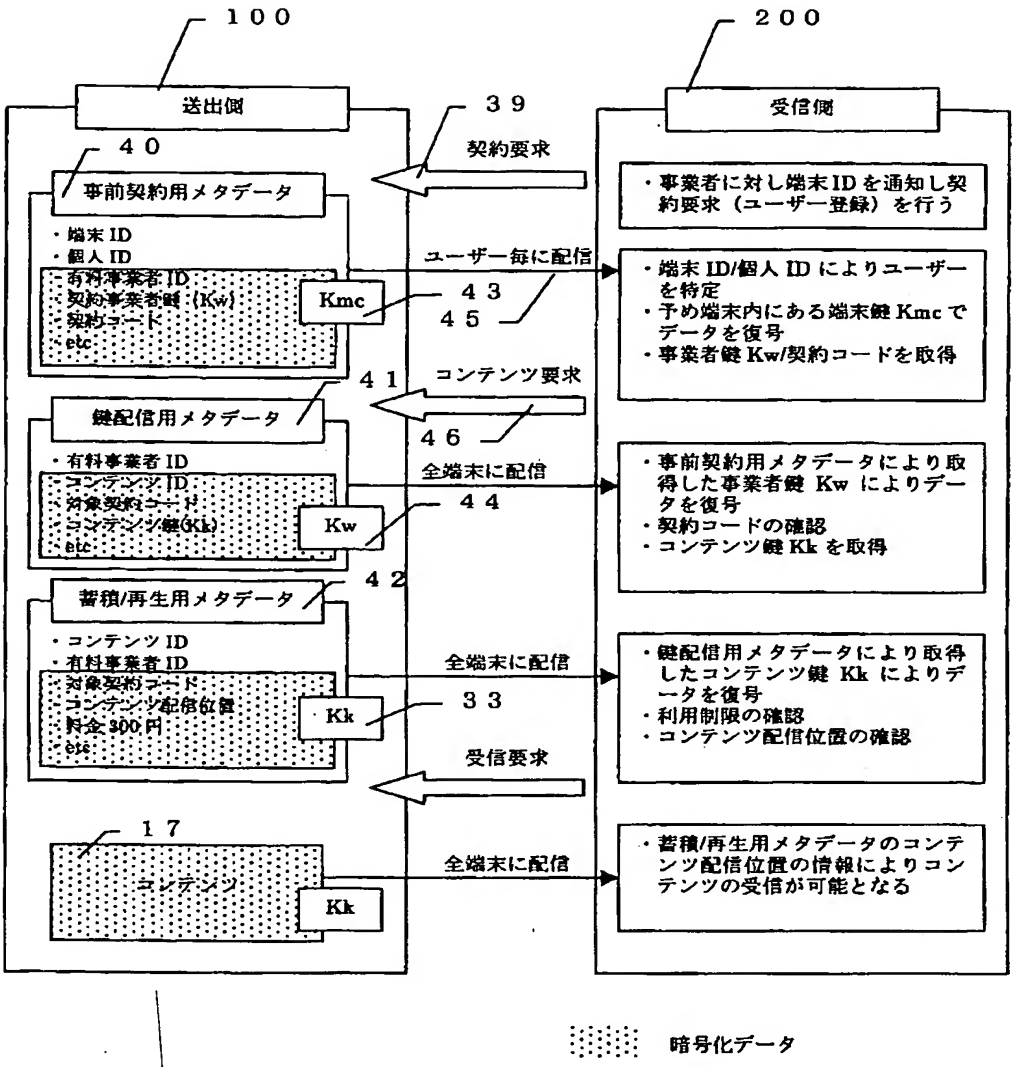
【図５】


TSP化
カルーセル化
31
32
33
34
Kk1
Kk2
MPEG2-Video(PES)
MPEG2-AAC(PES)
コンテンツ
BML
Text
JPEG
暗号化装置
コンテンツ内は同一鍵で暗号化
暗号化データ
映像系コンテンツ
データ系コンテンツ
27
28
29
30

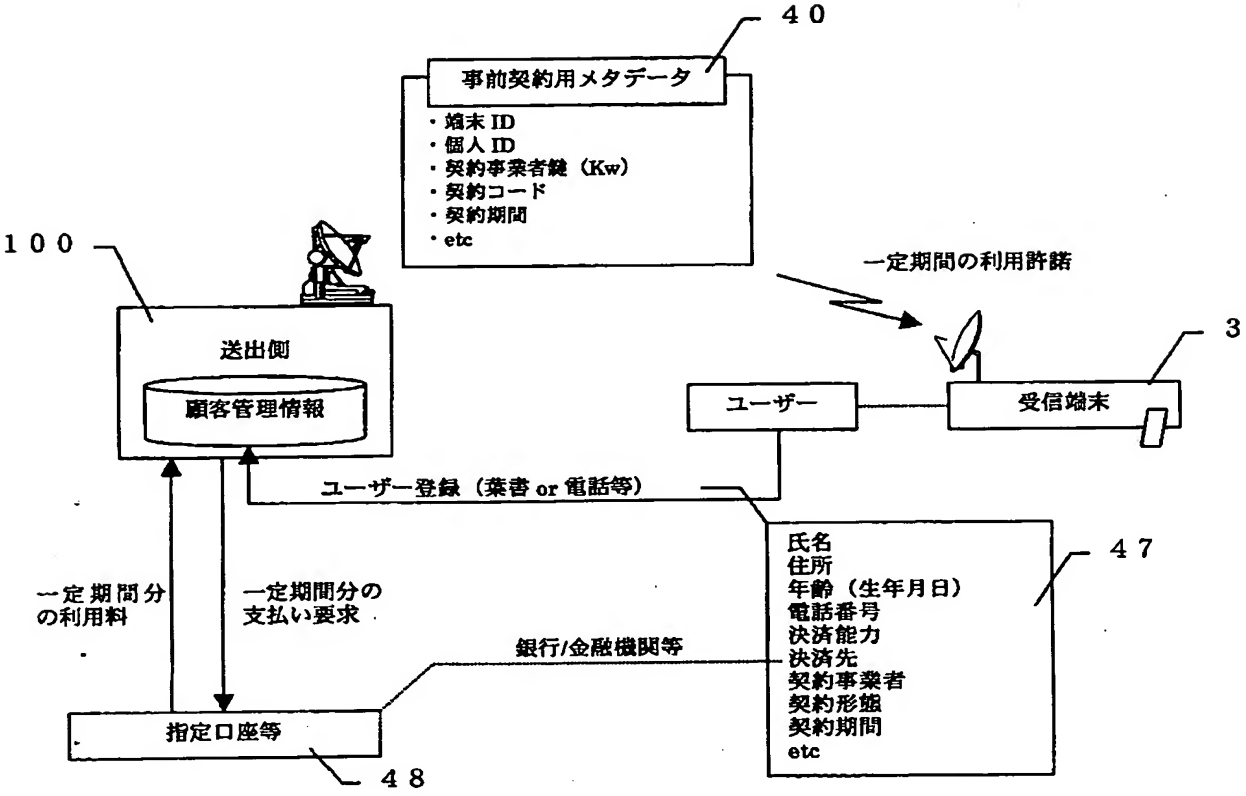
【図６】


非暗号化
部分
必要部分のみ
抽出し暗号化
暗号化
装置
暗号化
部分
暗号化データ
メタデータ
<metadata>
<meta_id> 0x00001 </meta_id>
<meta_type> 蓄積／再生用
</meta_type>
<meta_version> 0.01 </meta_version>
<content>
<content_id> 0x1234567 </content_id>
<暗号>
<利用制限>
<対象年齢> ２０歳以上 </対象年齢>
</利用制限>
<content 暗号化方式>
<方式> 著作権保護暗号 </化方式>
<key_id> kw_ID </key_id>
<コード> 0x11100111 </コード>
</content 暗号化方式>
<契約情報>
<契約 ID> 0x01 </契約 ID>
<契約 type> レンタル </契約 type>
<有効期限> ３日 </有効期限>
<料金> ３００円 </料金>
<課金 timing> 視聴時 </課金 timing>
</契約情報>
</暗号>
</content>
</metadata>
メタデータ
<metadata>
<meta_id> 0x00001 </meta_id>
<meta_type> 蓄積／再生用
</meta_type>
<meta_version> 0.01 </meta_version>
<content>
<content_id> 0x1234567 </content_id>
<暗号>
</暗号>
</content>
暗号化データ
<meta_id> 0x00001 </meta_id>
<meta_type> 暗号 </meta_type>
<暗号 length> xxxxbit </暗号 length>
35
36
37
38

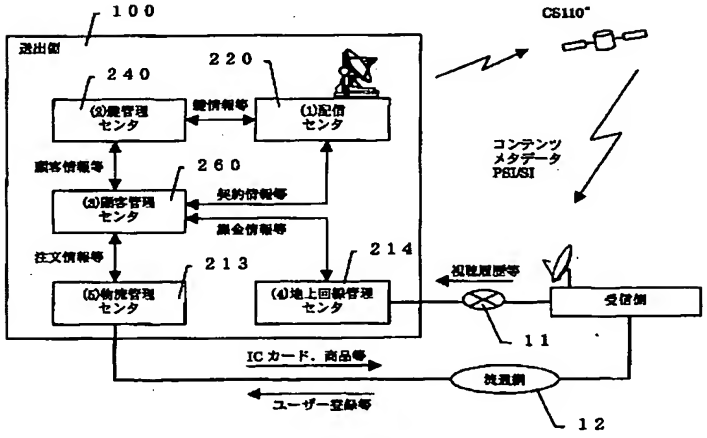
【図７】


１００
２００
送出側
受信側
３９
契約要求
４０
事前契約用メタデータ
・端末 ID
・個人 ID
・有料事業者 ID
・契約事業者鍵（Kw）
・契約コード
・etc
Kmc
ユーザー毎に配信
４３
４５
・事業者に対し端末 ID を通知し契約要求（ユーザー登録）を行う
・端末 ID/個人 ID によりユーザーを特定
・予め端末内にある端末鍵 Kmc でデータを復号
・事業者鍵 Kw/契約コードを取得
４１
コンテンツ要求
４６
鍵配信用メタデータ
・有料事業者 ID
・コンテンツ ID
・対象契約コード
・コンテンツ鍵(Kk)
・etc
Kw
全端末に配信
４４
・事前契約用メタデータにより取得した事業者鍵 Kw によりデータを復号
・契約コードの確認
・コンテンツ鍵 Kk を取得
４２
蓄積/再生用メタデータ
・コンテンツ ID
・有料事業者 ID
・対象契約コード
・コンテンツ配信位置
・料金 300 円
・etc
Kk
全端末に配信
３３
・鍵配信用メタデータにより取得したコンテンツ鍵 Kk によりデータを復号
・利用制限の確認
・コンテンツ配信位置の確認
受信要求
１７
コンテンツ
Kk
全端末に配信
・蓄積/再生用メタデータのコンテンツ配信位置の情報によりコンテンツの受信が可能となる
暗号化データ

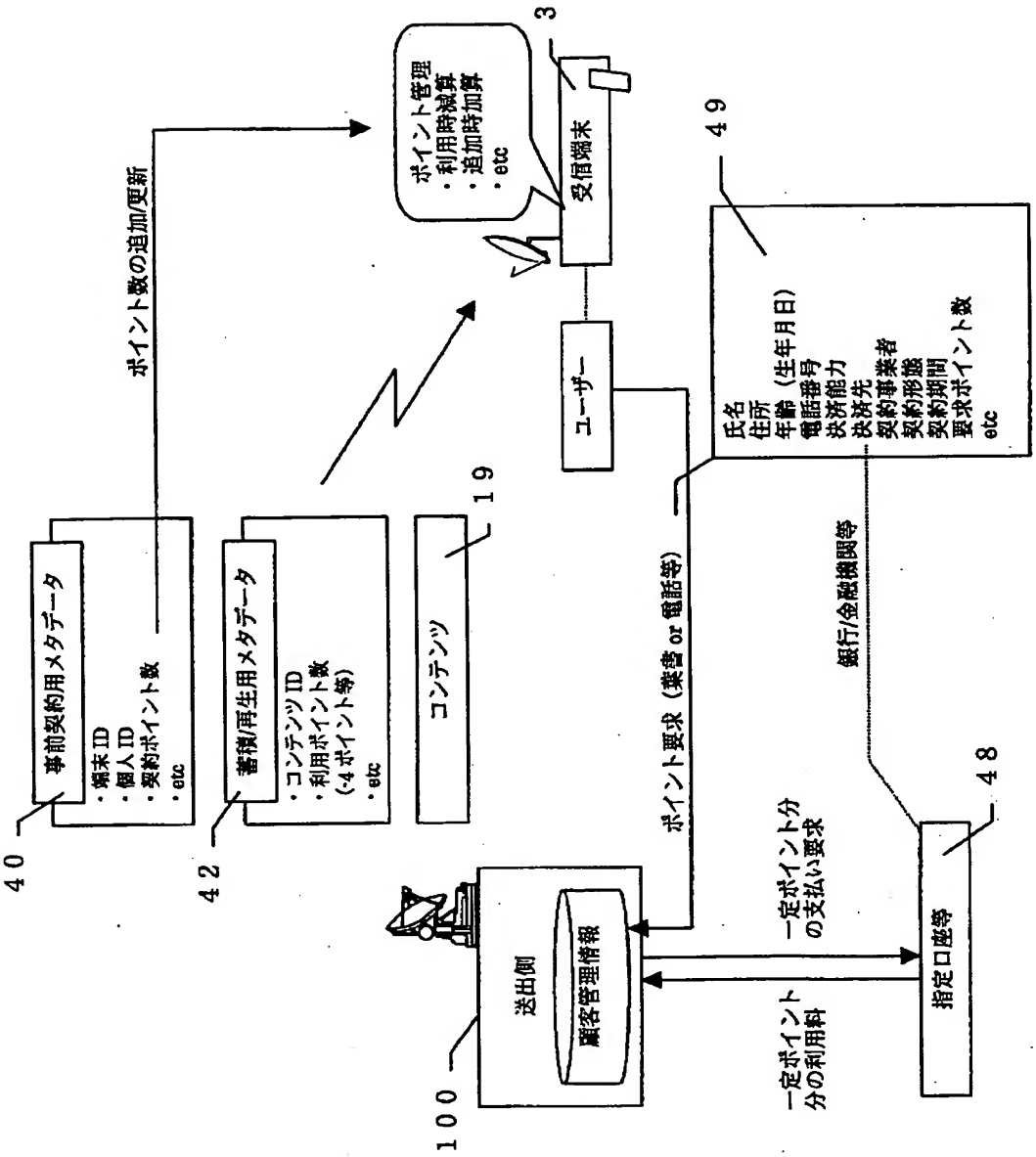
【図８】


４０
事前契約用メタデータ
・端末 ID
・個人 ID
・契約事業者鍵（Kw）
・契約コード
・契約期間
・etc
１００
送出側
顧客管理情報
一定期間の利用許諾
３
ユーザー
受信端末
ユーザー登録（葉書 or 電話等）
氏名
住所
年齢（生年月日）
電話番号
決済能力
決済先
契約事業者
契約形態
契約期間
etc
４７
一定期間分の利用料
一定期間分の支払い要求
銀行/金融機関等
指定口座等
４８

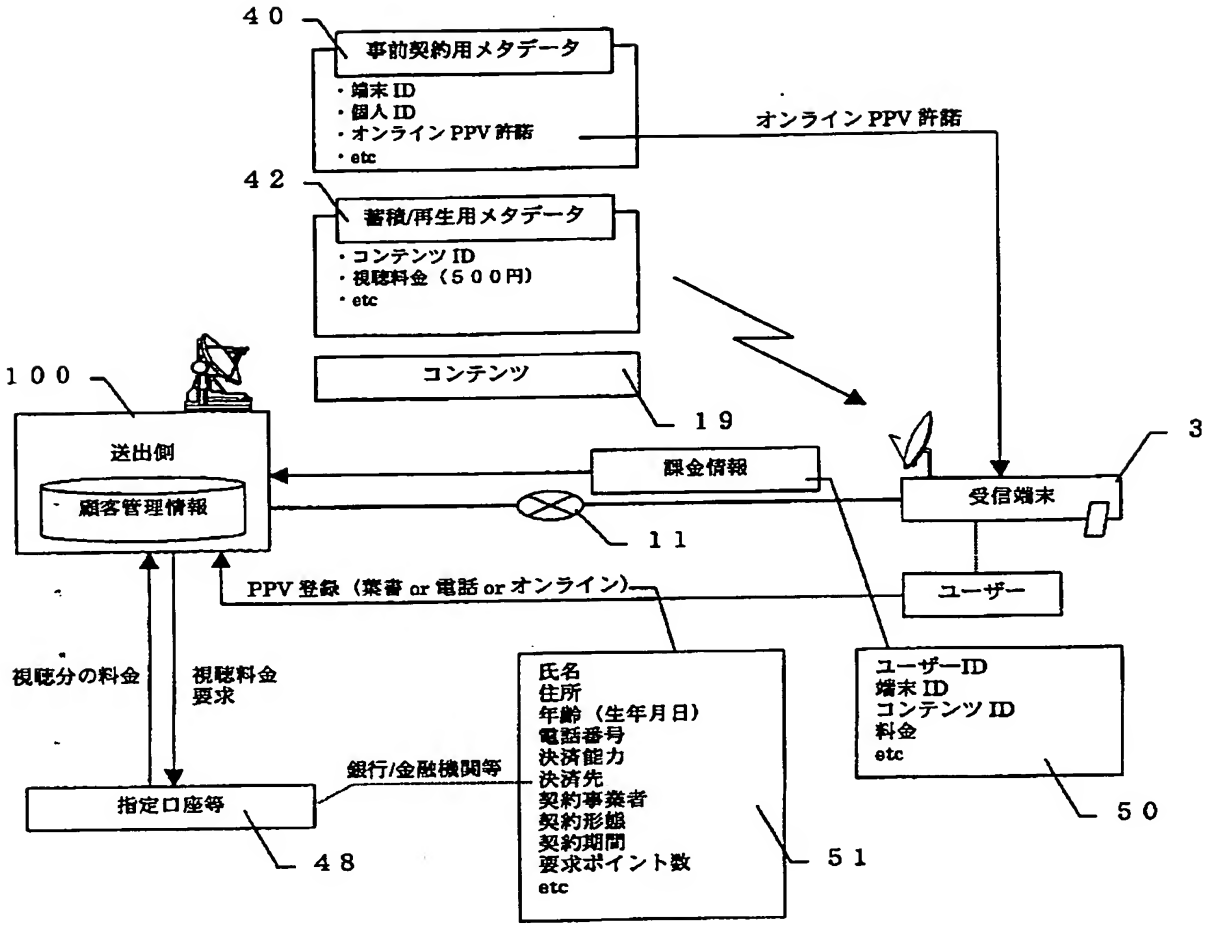
【図１５】


１００
送出側
２２０
２４０
(2)鍵管理センタ
鍵情報等
(1)配信センタ
顧客情報等
２６０
(3)顧客管理センタ
契約情報等
課金情報等
注文情報等
２１３
２１４
(5)物流管理センタ
(4)地上回線管理センタ
視聴履歴等
CS110°
コンテンツ
メタデータ
PSI/SI
受信側
１１
ICカード、商品等
ユーザー登録等
放送網
１２

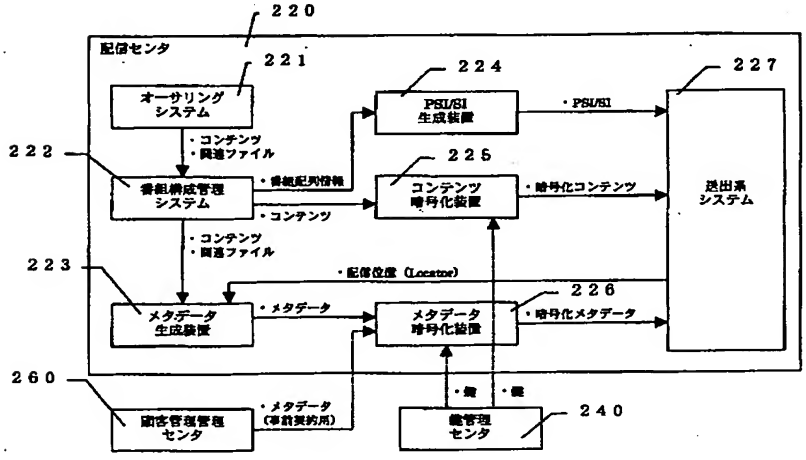
【図９】


ポイント管理
・利用時減算
・追加時加算
・etc
3
受信端末
ユーザー
49
氏名
住所
年齢（生年月日）
電話番号
決済能力
決済先
契約事業者
契約形態
契約期間
要求ポイント数
etc
ポイント数の追加/更新
事前契約用メタデータ
・端末ID
・個人ID
・契約ポイント数
・etc
40
蓄積/再生用メタデータ
・コンテンツID
・利用ポイント数
（4ポイント等）
・etc
42
コンテンツ
19
ポイント要求（業書 or 電話等）
銀行/金融機関等
一定ポイント分
の支払い要求
一定ポイント
分の利用料
48
指定口座等
送出側
顧客管理情報
100

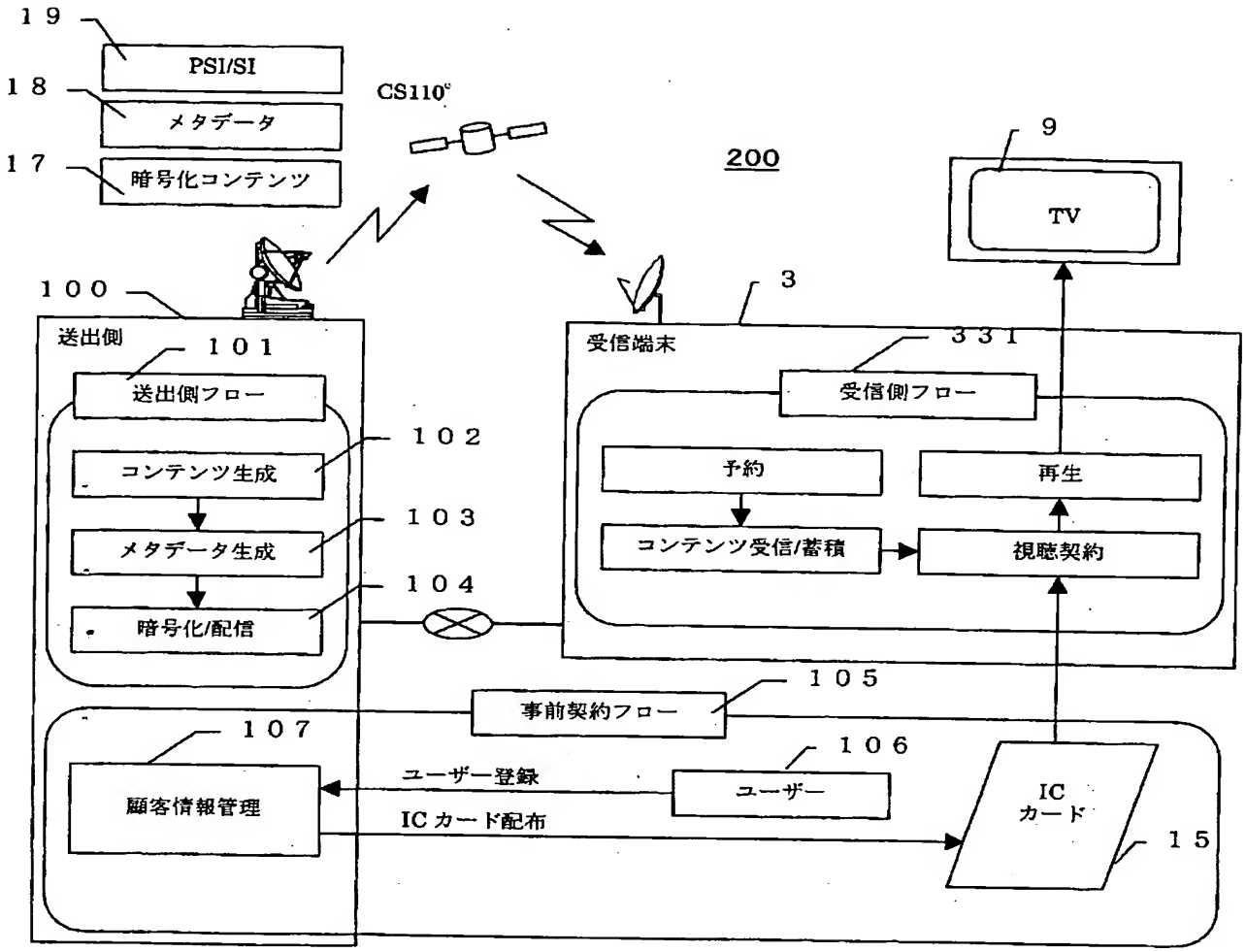
【図１０】


４０
事前契約用メタデータ
・端末ID
・個人ID
・オンラインPPV許諾
・etc
オンラインPPV許諾
４２
蓄積/再生用メタデータ
・コンテンツID
・視聴料金（５００円）
・etc
コンテンツ
１９
１００
送出側
顧客管理情報
課金情報
１１
３
受信端末
PPV登録（葉書 or 電話 or オンライン）
ユーザー
視聴分の料金
視聴料金
要求
氏名
住所
年齢（生年月日）
電話番号
決済能力
決済先
契約事業者
契約形態
契約期間
要求ポイント数
etc
銀行/金融機関等
ユーザーID
端末ID
コンテンツID
料金
etc
５０
指定口座等
４８
５１

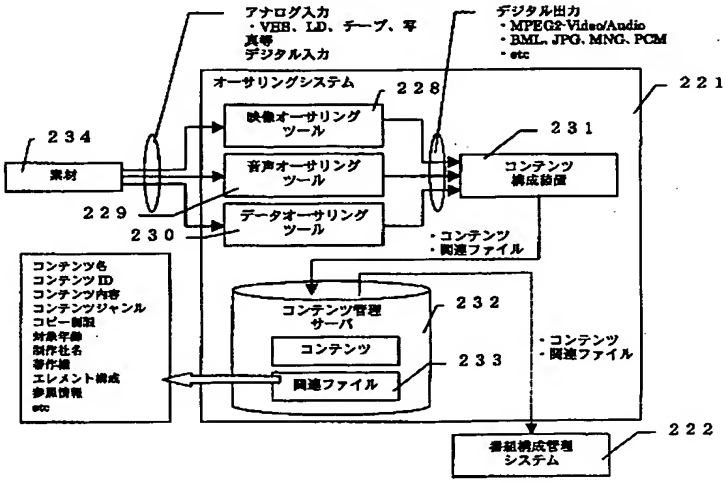
【図１６】


２２０
配信センタ
２２１
オーサリングシステム
２２４
PSI/SI生成装置
・PSI/SI
２２７
・コンテンツ
・関連ファイル
２２２
番組構成管理システム
・番組記列情報
２２５
コンテンツ暗号化装置
・暗号化コンテンツ
送出系システム
・コンテンツ
・コンテンツ
・関連ファイル
２２３
・配信位置（Locator）
２２６
メタデータ生成装置
・メタデータ
メタデータ暗号化装置
・暗号化メタデータ
２６０
顧客管理管理センタ
・メタデータ（事前契約用）
・鍵
・鍵
２４０
鍵管理センタ

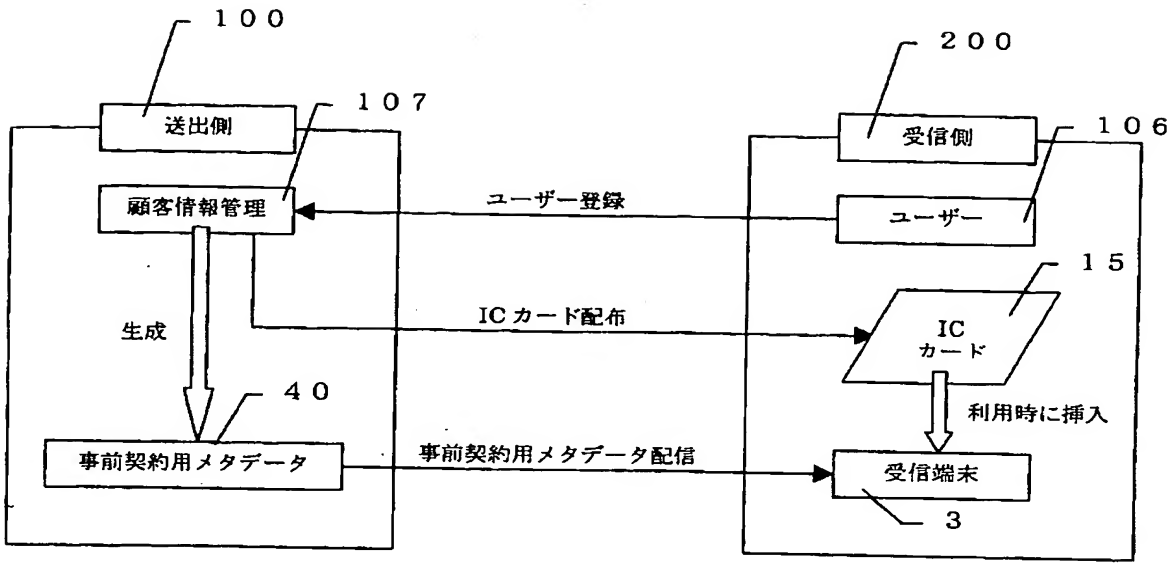
【図１１】


１９
PSI/SI
１８
メタデータ
１７
暗号化コンテンツ
CS110°
200
9
TV
１００
送出側
１０１
送出側フロー
１０２
コンテンツ生成
１０３
メタデータ生成
１０４
暗号化/配信
3
受信端末
３３１
受信側フロー
予約
再生
コンテンツ受信/蓄積
視聴契約
１０５
事前契約フロー
１０７
顧客情報管理
ユーザー登録
１０６
ユーザー
ICカード配布
IC
カード
１５

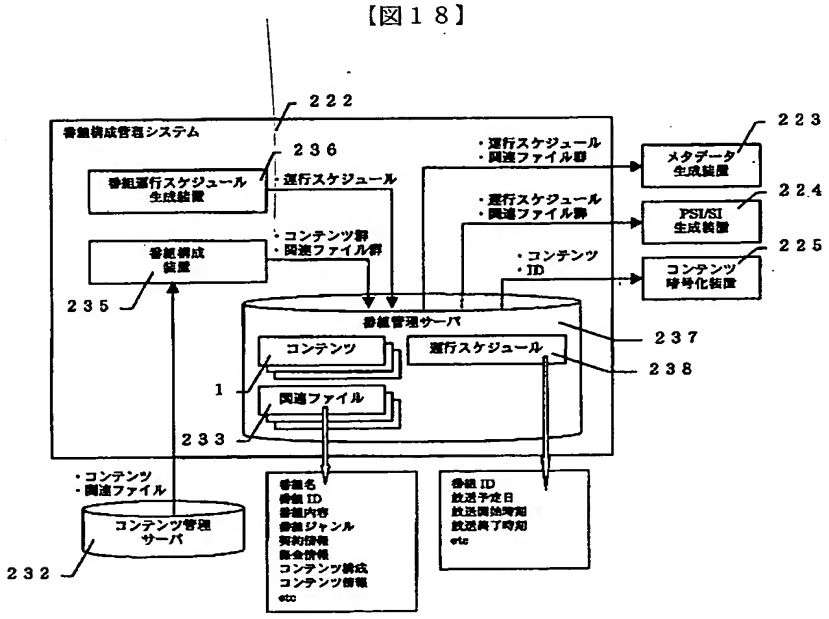
【図１７】


アナログ入力
・VHS、LD、テープ、写真等
デジタル入力
デジタル出力
・MPEG2-Video/Audio
・BML、JPG、MNG、PCM
・etc
オーサリングシステム
２２８
２２１
２３４
素材
映像オーサリングツール
音声オーサリングツール
データオーサリングツール
２３１
コンテンツ構成設定
２２９
２３０
・コンテンツ
・関連ファイル
コンテンツ名
コンテンツID
コンテンツ内容
コンテンツジャンル
コピー制御
対象年齢
制作社名
著作権
エレメント構成
参照情報
etc
コンテンツ管理サーバ
２３２
コンテンツ
２３３
関連ファイル
・コンテンツ
・関連ファイル
２２２
番組構成管理システム

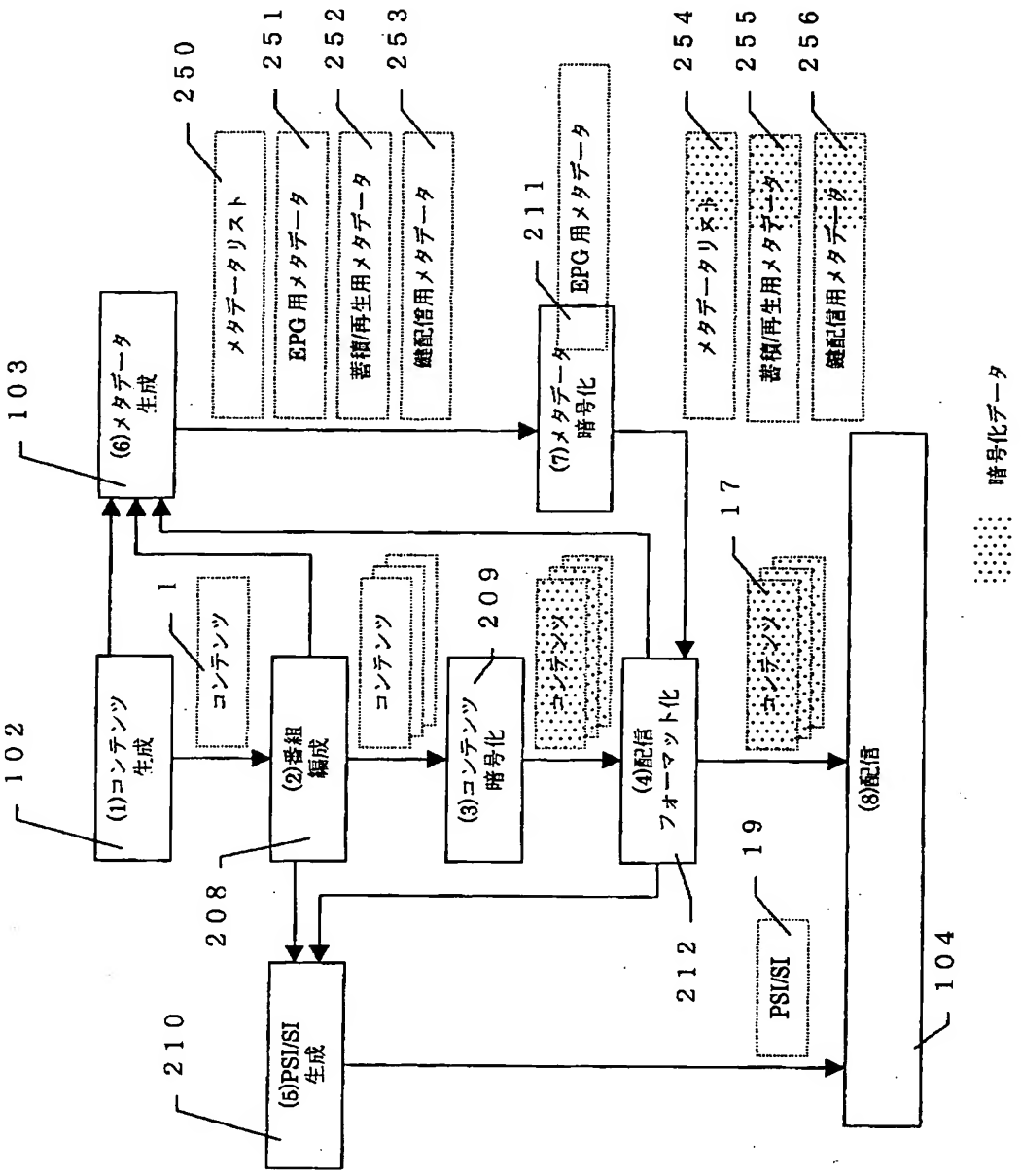
【図１２】


１００
送出側
１０７
顧客情報管理
生成
４０
事前契約用メタデータ
ユーザー登録
ICカード配布
事前契約用メタデータ配信
２００
受信側
１０６
ユーザー
１５
IC
カード
利用時に挿入
受信端末
３

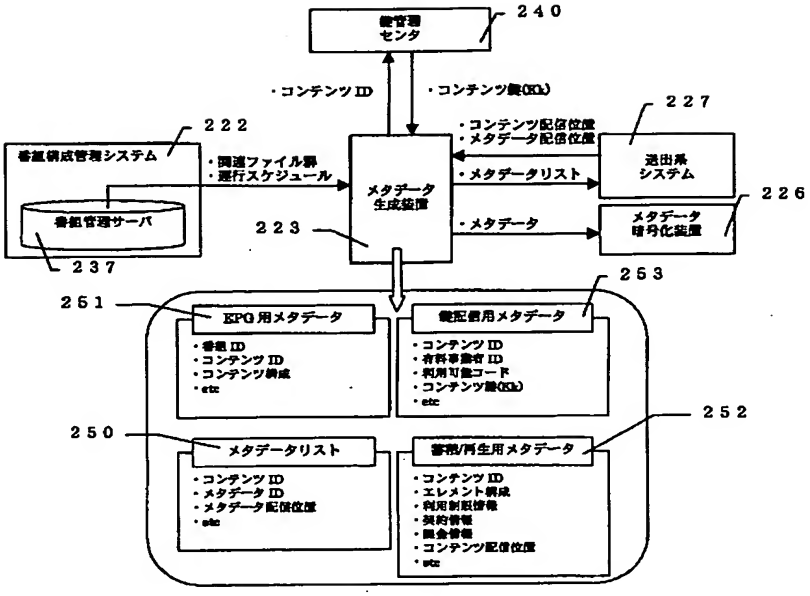
【図１８】


２２２
番組構成管理システム
２３６
番組運行スケジュール生成装置
・運行スケジュール
・コンテンツ群
・関連ファイル群
番組構成装置
２３５
・運行スケジュール
・関連ファイル群
２２３
メタデータ生成装置
・運行スケジュール
・関連ファイル群
２２４
PSI/SI生成装置
・コンテンツ
・ID
２２５
コンテンツ暗号化装置
番組管理サーバ
２３７
コンテンツ
運行スケジュール
２３８
１
関連ファイル
２３３
・コンテンツ
・関連ファイル
コンテンツ管理サーバ
２３２
番組名
番組ID
番組内容
番組ジャンル
契約情報
集金情報
コンテンツ構成
コンテンツ情報
etc
番組ID
放送予定日
放送開始時刻
放送終了時刻
etc

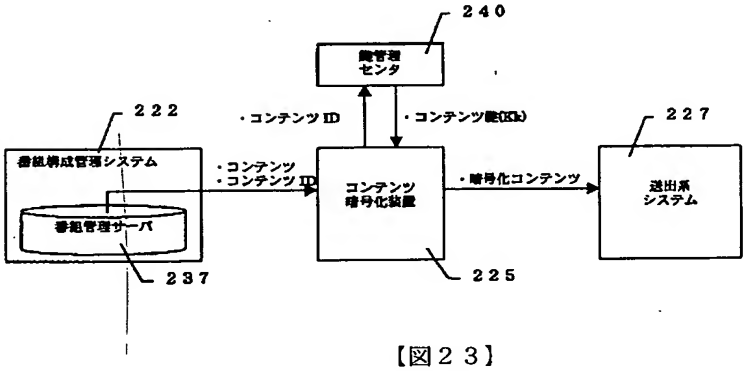
【図１３】


250
251
252
253
254
255
256
メタデータリスト
EPG用メタデータ
蓄積/再生用メタデータ
鍵配信用メタデータ
211
EPG用メタデータ
メタデータリスト
蓄積/再生用メタデータ
鍵配信用メタデータ
103
(6)メタデータ生成
(7)メタデータ暗号化
17
1
コンテンツ
102
(1)コンテンツ生成
(2)番組編成
209
(3)コンテンツ暗号化
(4)配信フォーマット化
(8)配信
208
212
19
PSI/SI
104
210
(5)PSI/SI生成
暗号化データ

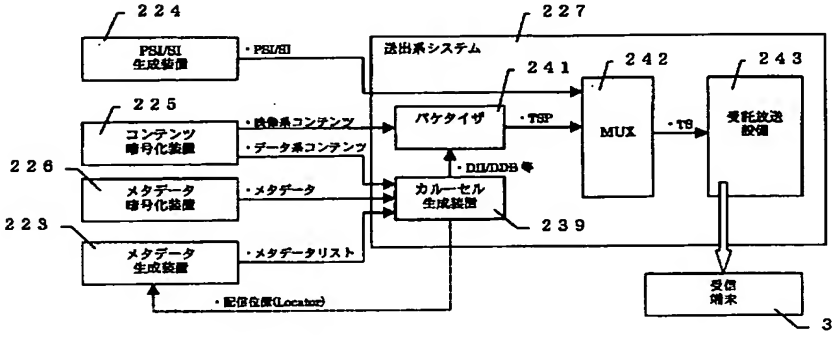
【図２０】


鍵管理センタ
240
・コンテンツID
・コンテンツ鍵(Kk)
222
番組構成管理システム
・関連ファイル群
・運行スケジュール
番組管理サーバ
237
メタデータ生成装置
223
・コンテンツ配信位置
・メタデータ配信位置
・メタデータリスト
・メタデータ
227
送出系システム
226
メタデータ暗号化装置
253
251
EPG用メタデータ
・番組ID
・コンテンツID
・コンテンツ構成
・etc
鍵配信用メタデータ
・コンテンツID
・有料事業者ID
・利用可能コード
・コンテンツ鍵(Kk)
・etc
252
250
メタデータリスト
・コンテンツID
・メタデータID
・メタデータ配信位置
・etc
蓄積/再生用メタデータ
・コンテンツID
・エレメント構成
・利用制限情報
・契約情報
・課金情報
・コンテンツ配信位置
・etc

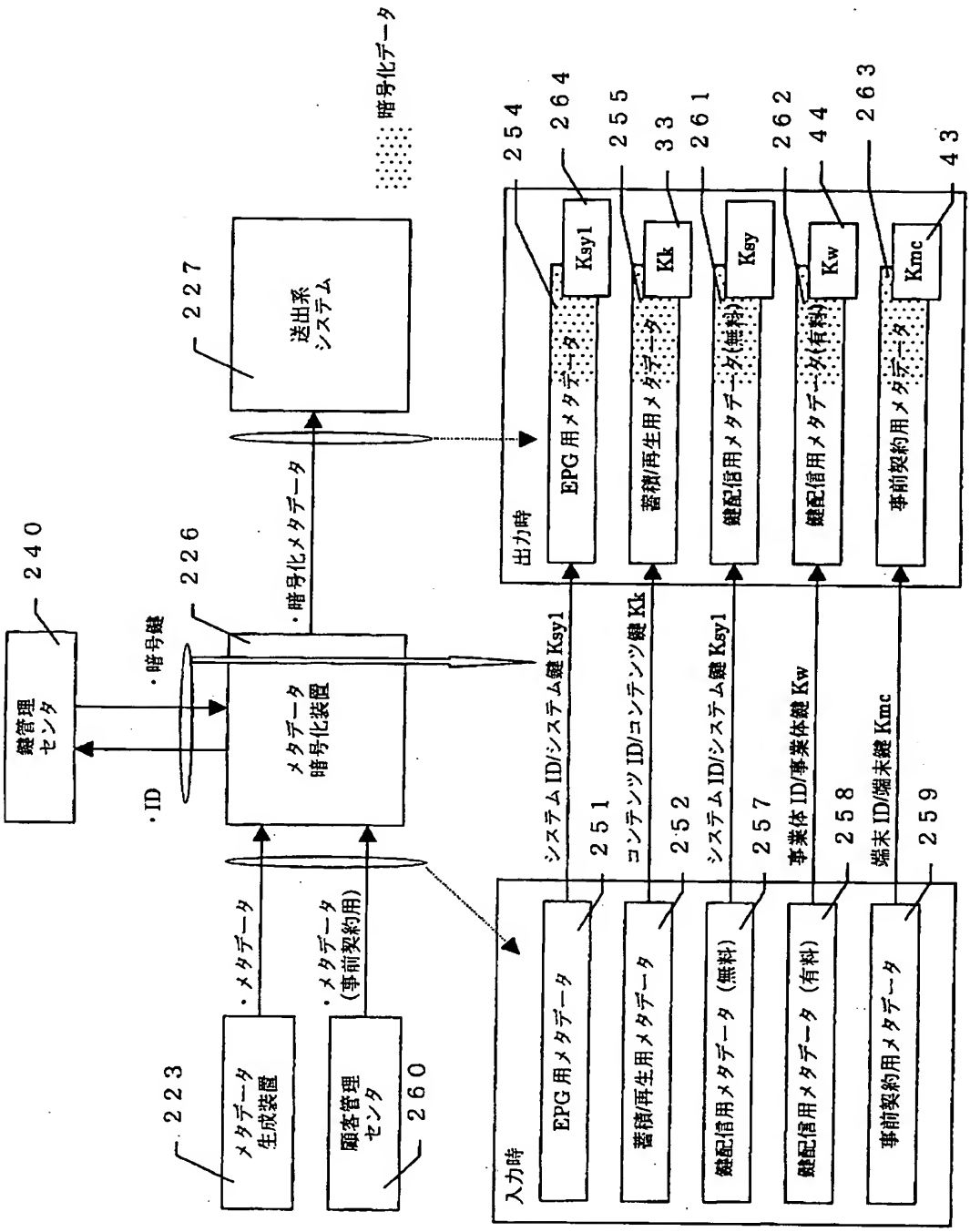
【図２１】


240
鍵管理センタ
222
番組構成管理システム
・コンテンツID
・コンテンツ鍵(Kk)
227
・コンテンツ
・コンテンツID
コンテンツ暗号化装置
・暗号化コンテンツ
送出系システム
番組管理サーバ
237
225

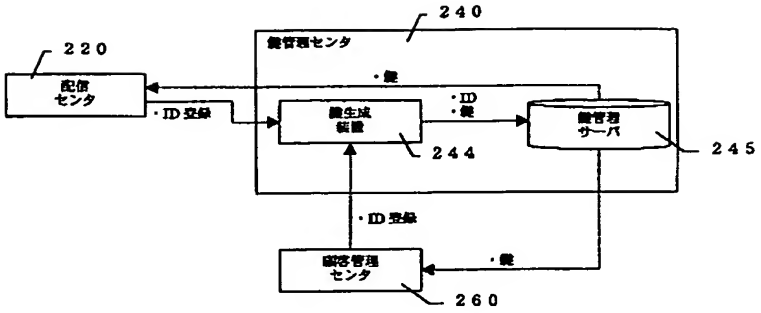
【図２３】


224
PSI/SI生成装置
・PSI/SI
227
送出系システム
241
242
243
225
コンテンツ暗号化装置
・映像系コンテンツ
・データ系コンテンツ
パケタイザ
・TSP
MUX
・TS
受託放送設備
・DII/DDB等
226
メタデータ暗号化装置
・メタデータ
カルーセル生成装置
239
223
メタデータ生成装置
・メタデータリスト
・配信位置(Locator)
受信端末
3

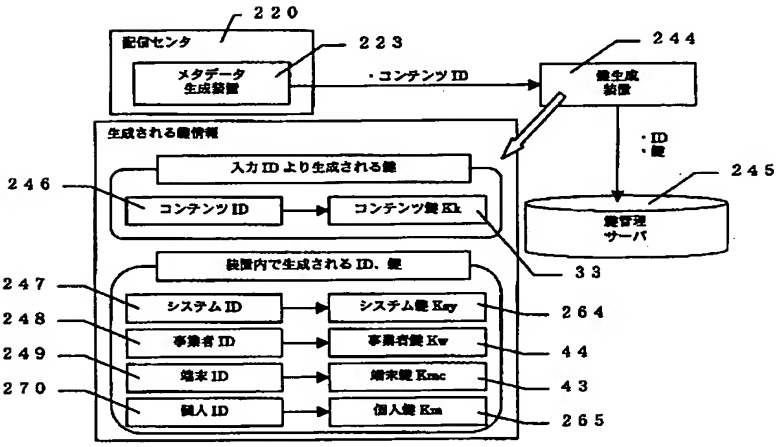
【図２２】


暗号化データ
送出系システム
227
240
鍵管理センタ
・暗号鍵
・ID
226
メタデータ暗号化装置
・暗号化メタデータ
・メタデータ
・メタデータ(事前契約用)
223
メタデータ生成装置
260
顧客管理センタ
254
出力時
264
255
33
261
262
44
263
43
EPG用メタデータ
Ksy1
蓄積/再生用メタデータ
Kk
鍵配信用メタデータ(無料)
Ksy
鍵配信用メタデータ(有料)
Kw
事前契約用メタデータ
Kmc
システムID/システム鍵Ksy1
コンテンツID/コンテンツ鍵Kk
システムID/システム鍵Ksy1
事業体ID/事業体鍵Kw
端末ID/端末鍵Kmc
入力時
251
252
257
258
259
EPG用メタデータ
蓄積/再生用メタデータ
鍵配信用メタデータ（無料）
鍵配信用メタデータ（有料）
事前契約用メタデータ

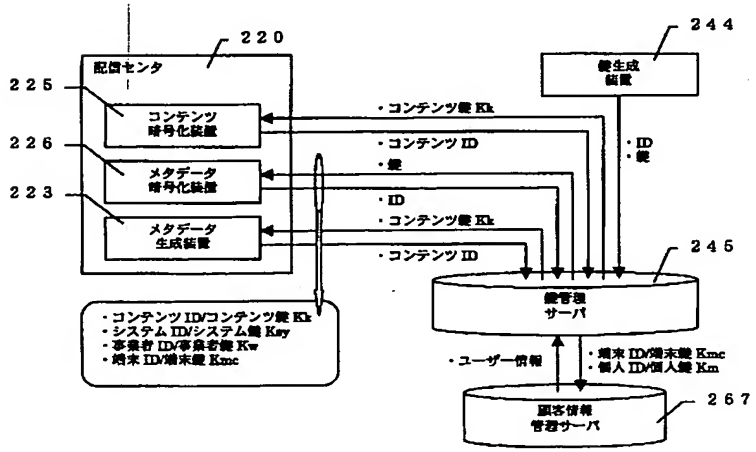
【図２４】


240
鍵管理センタ
220
配信センタ
・鍵
・ID登録
鍵生成装置
・ID
・鍵
鍵管理サーバ
244
245
・ID登録
顧客管理センタ
・鍵
260

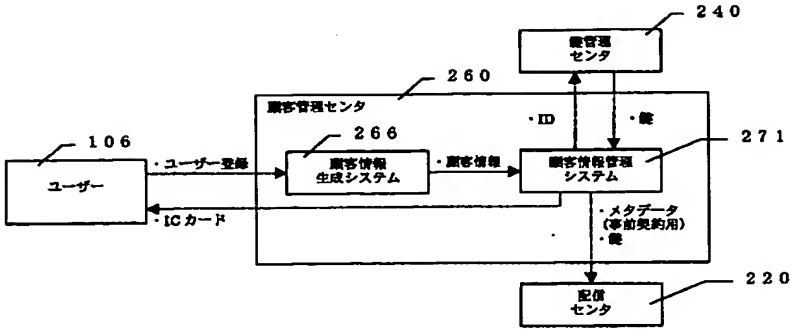
【図２５】


220
配信センタ
223
メタデータ生成装置
・コンテンツID
244
鍵生成装置
・ID
・鍵
245
鍵管理サーバ
生成される鍵情報
入力IDより生成される鍵
246
コンテンツID
コンテンツ鍵Kk
33
装置内で生成されるID、鍵
247
システムID
システム鍵Ksy
264
248
事業者ID
事業者鍵Kw
44
249
端末ID
端末鍵Kmc
43
270
個人ID
個人鍵Km
265

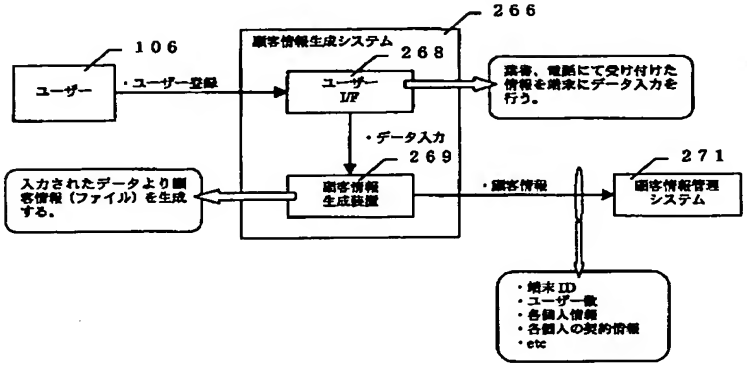
【図２６】


220
配信センタ
244
鍵生成装置
225
コンテンツ暗号化装置
・コンテンツ鍵Kk
226
メタデータ暗号化装置
・コンテンツID
・鍵
・ID/鍵
223
メタデータ生成装置
・ID
・コンテンツ鍵Kk
・コンテンツID
245
鍵管理サーバ
・コンテンツID/コンテンツ鍵Kk
・システムID/システム鍵Ksy
・事業者ID/事業者鍵Kw
・端末ID/端末鍵Kmc
・ユーザー情報
・端末ID/端末鍵Kmc
・個人ID/個人鍵Km
267
顧客情報管理サーバ

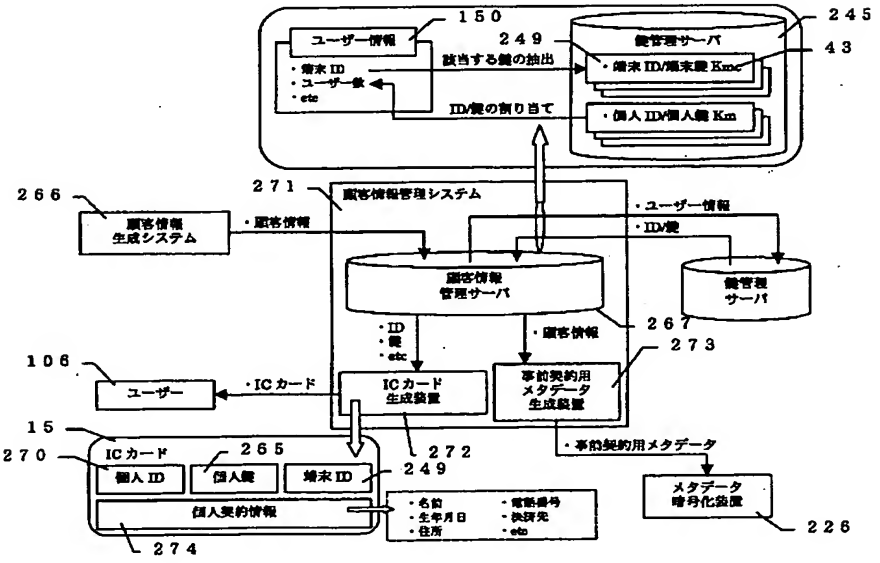
【図２７】


240
鍵管理センタ
260
顧客管理センタ
・ID
・鍵
106
ユーザー
・ユーザー登録
266
顧客情報生成システム
・顧客情報
271
顧客情報管理システム
・ICカード
・メタデータ（事前契約用）
・鍵
220
配信センタ

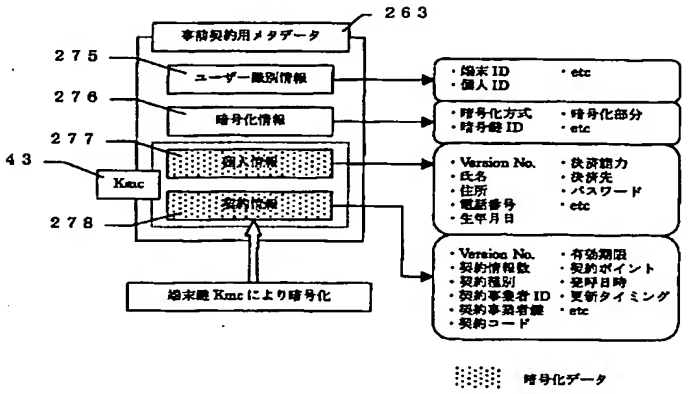
【図２８】


266
顧客情報生成システム
106
ユーザー
・ユーザー登録
268
ユーザーI/F
端末、電話にて受け付けた情報を端末にデータ入力を行う。
・データ入力
269
顧客情報生成装置
入力されたデータより顧客情報（ファイル）を生成する。
・顧客情報
271
顧客情報管理システム
・端末ID
・ユーザー数
・各個人情報
・各個人の契約情報
・etc

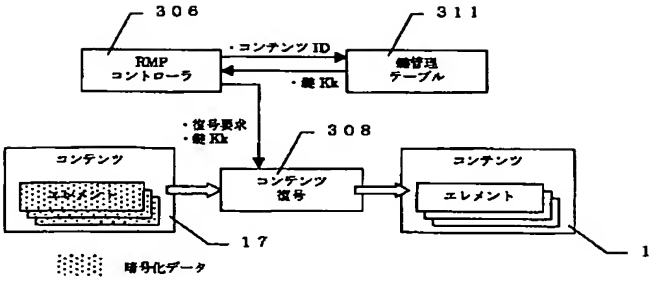
【図２９】


150
ユーザー情報
・端末ID
・ユーザー数
・etc
249
該当する鍵の抽出
ID/鍵の割り当て
245
鍵管理サーバ
43
・端末ID/端末鍵 Kmc
・個人ID/個人鍵 Km
266
顧客情報生成システム
・顧客情報
271
顧客情報管理システム
・ユーザー情報
・ID/鍵
顧客情報管理サーバ
鍵管理サーバ
・ID
・鍵
・etc
・顧客情報
267
273
106
ユーザー
・ICカード
ICカード生成装置
事前契約用メタデータ生成装置
15
ICカード
270
個人ID
265
個人鍵
端末ID
272
249
・事前契約用メタデータ
個人契約情報
・名前
・生年月日
・住所
・電話番号
・決済先
・etc
メタデータ暗号化装置
226
274

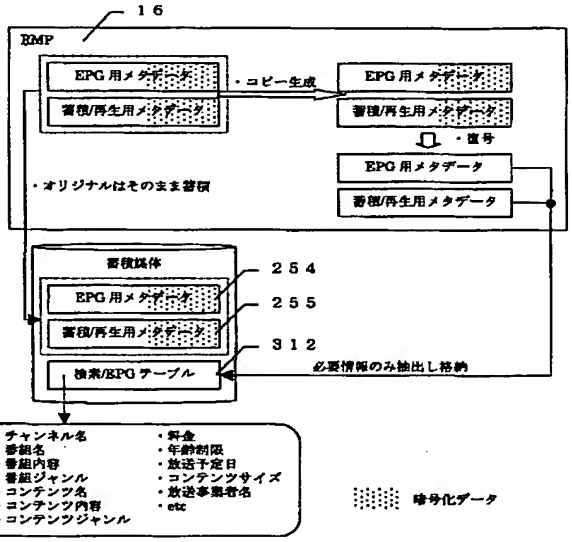
【図３０】



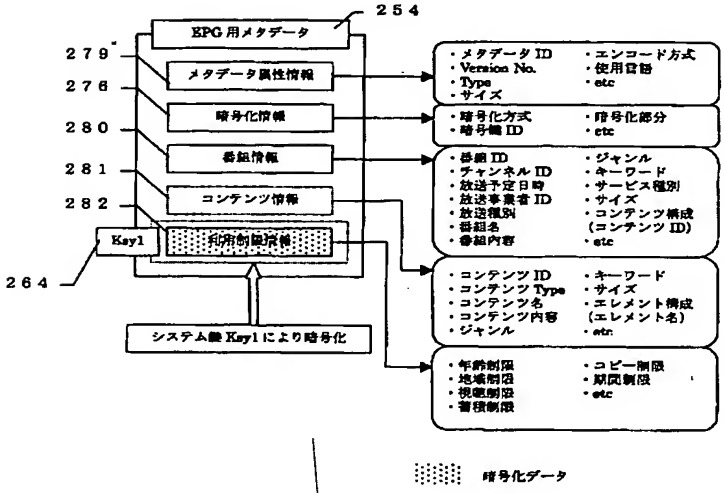
【図３８】



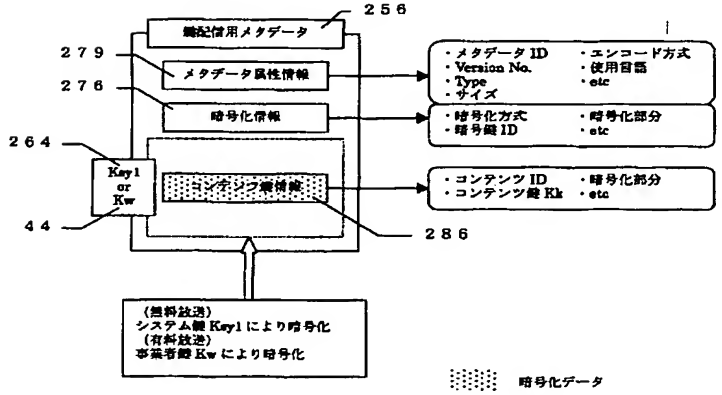
【図４６】



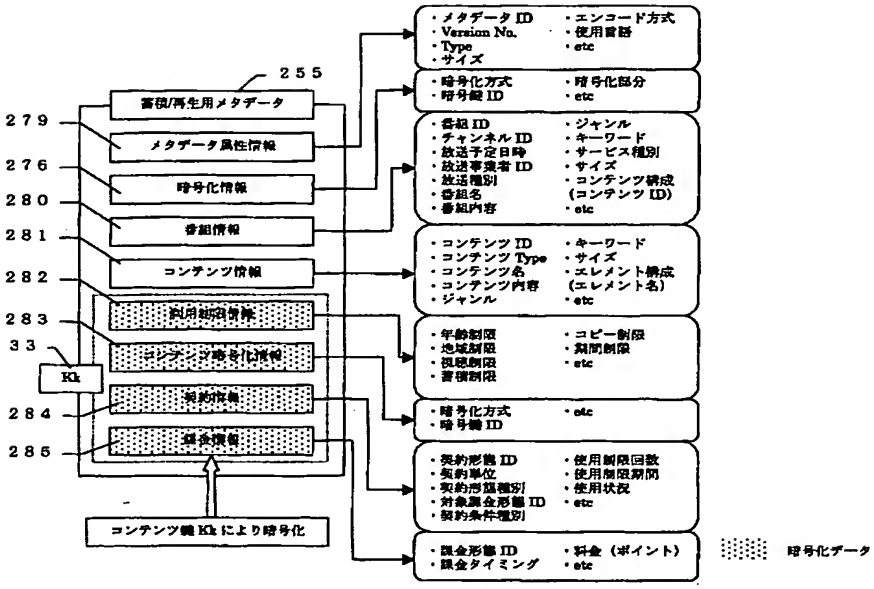
【図３１】



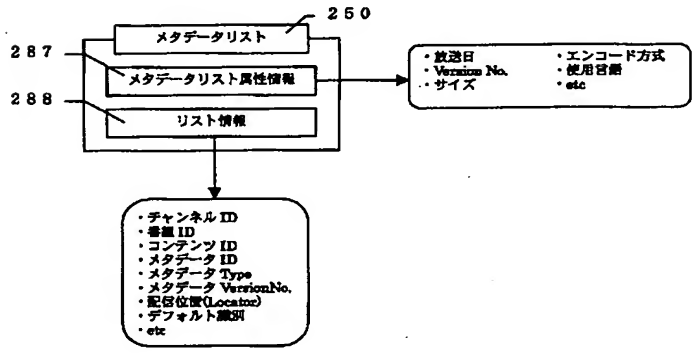
【図３３】



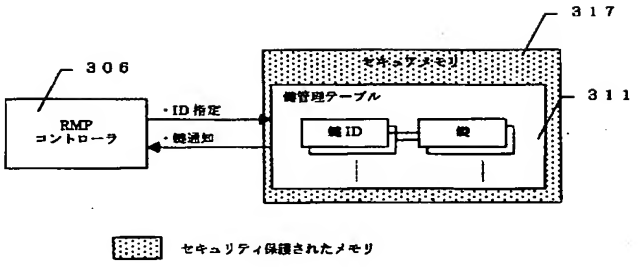
【図３２】



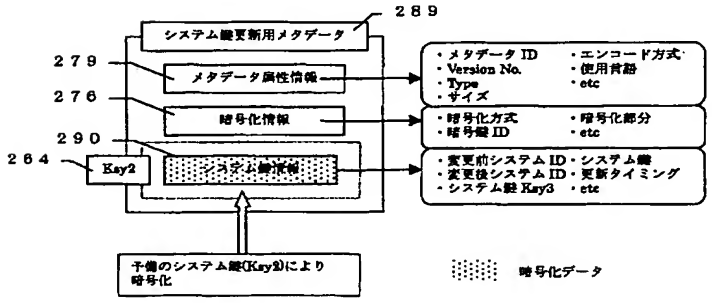
【図３４】



【図４０】



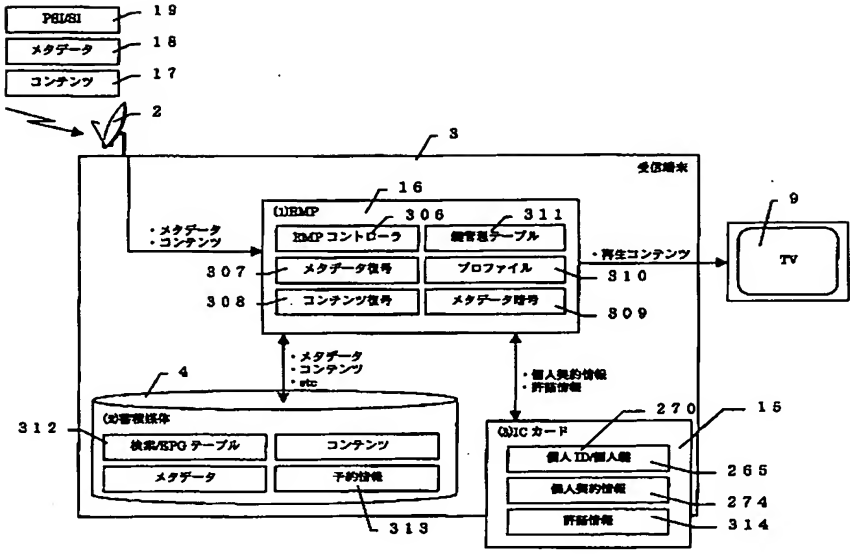
【図３５】



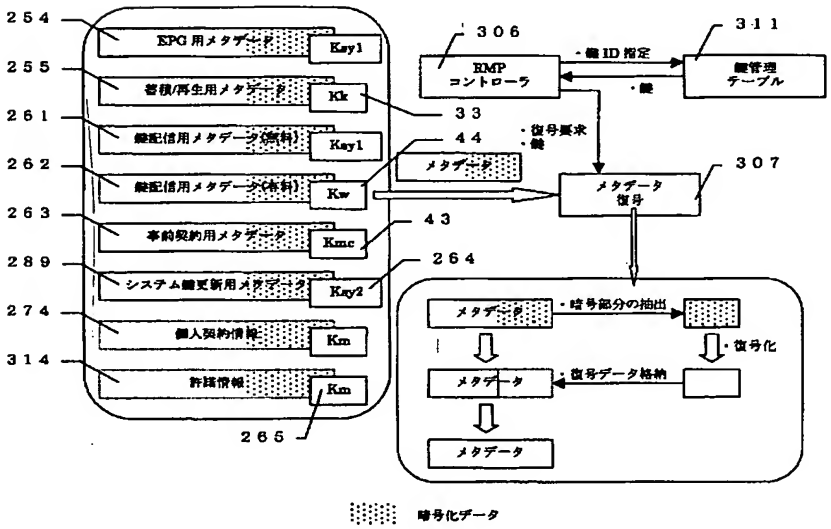
【図５０】

コンテンツ種別	エレメント
映像系コンテンツ	・MPEG2-Video stream(PES) ・MPEG2-Audio stream(PES) ・MPEG1-Video stream(PES) ・その他
データ系コンテンツ	・BML ・XML ・Text ・JPG ・MNG ・MPEG2-Video ・MPEG2-Audio ・MPEG1-Video ・MPEG1-PS ・MPEG2-PS ・その他

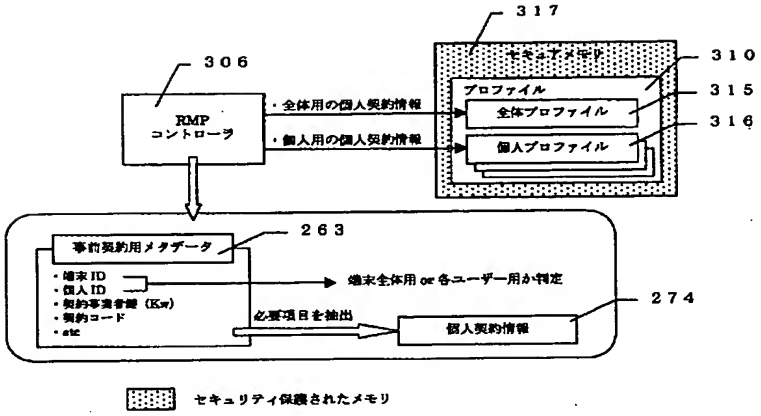
【図３６】


PSI/SI
メタデータ
コンテンツ
19
18
17
2
3
受信端末
16
(1)RMP
306
311
RMPコントローラ
鍵管理テーブル
307
メタデータ復号
プロファイル
308
コンテンツ復号
メタデータ暗号
309
310
・メタデータ
・コンテンツ
・再生コンテンツ
9
TV
・メタデータ
・コンテンツ
・etc
・個人契約情報
・許諾情報
4
(4)蓄積媒体
312
検索/EPGテーブル
コンテンツ
メタデータ
予約情報
313
(3)ICカード
270
15
個人ID/個人鍵
265
個人契約情報
274
許諾情報
314

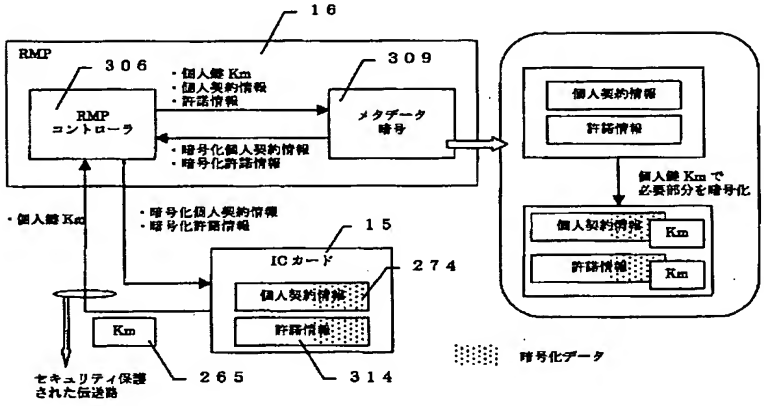
【図３７】


254
EPG用メタデータ
Key1
255
蓄積/再生用メタデータ
Kk
261
鍵配信用メタデータ(無料)
Key1
262
鍵配信用メタデータ(有料)
Kw
263
事前契約用メタデータ
Kmc
289
システム鍵更新用メタデータ
Key2
274
個人契約情報
Km
314
許諾情報
Km
265
33
44
43
264
306
311
RMP
コントローラ
・鍵ID指定
・鍵
鍵管理
テーブル
・復号要求
・鍵
メタデータ
307
メタデータ
復号
メタデータ
・暗号部分の抽出
・復号化
メタデータ
・復号データ格納
メタデータ
暗号化データ

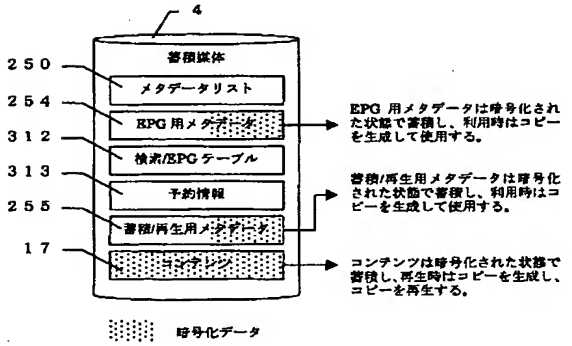
【図３９】


３１７
セキュアメモリ
３１０
プロファイル
３１５
全体プロファイル
３１６
個人プロファイル
３０６
RMP
コントローラ
・全体用の個人契約情報
・個人用の個人契約情報
２６３
事前契約用メタデータ
・端末ID
・個人ID
・契約事業者鍵（Ksv）
・契約コード
・etc
端末全体用 or 各ユーザー用か判定
必要項目を抽出
２７４
個人契約情報
セキュリティ保護されたメモリ

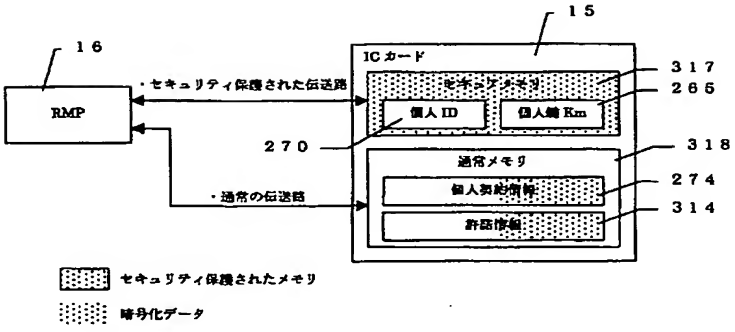
【図４１】


１６
RMP
３０６
RMP
コントローラ
・個人鍵 Km
・個人契約情報
・許諾情報
３０９
メタデータ
暗号
・暗号化個人契約情報
・暗号化許諾情報
個人契約情報
許諾情報
個人鍵 Km で
必要部分を暗号化
個人契約情報
Km
許諾情報
Km
・個人鍵 Km
・暗号化個人契約情報
・暗号化許諾情報
１５
ICカード
２７４
個人契約情報
許諾情報
Km
２６５
３１４
セキュリティ保護
された伝送路
暗号化データ

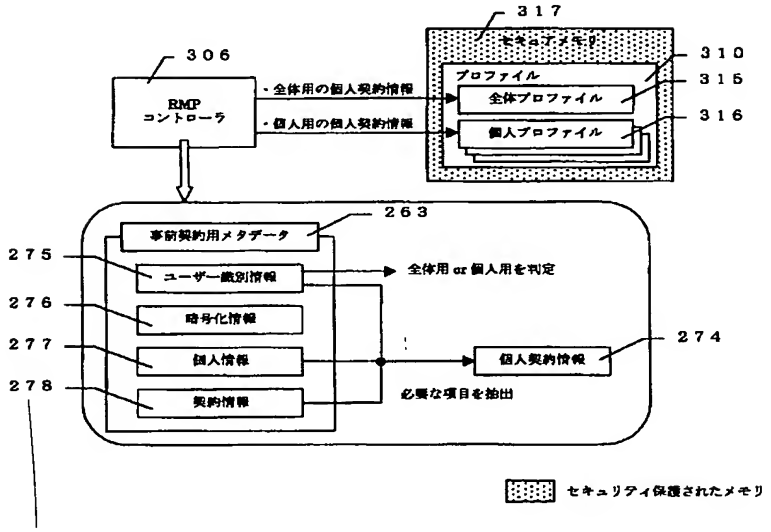
【図４２】


４
２５０
蓄積媒体
メタデータリスト
２５４
EPG 用メタデータ
３１２
検索/EPG テーブル
３１３
予約情報
２５５
蓄積/再生用メタデータ
１７
コンテンツ
EPG 用メタデータは暗号化された状態で蓄積し、利用時はコピーを生成して使用する。
蓄積/再生用メタデータは暗号化された状態で蓄積し、利用時はコピーを生成して使用する。
コンテンツは暗号化された状態で蓄積し、再生時はコピーを生成し、コピーを再生する。
暗号化データ

【図４３】



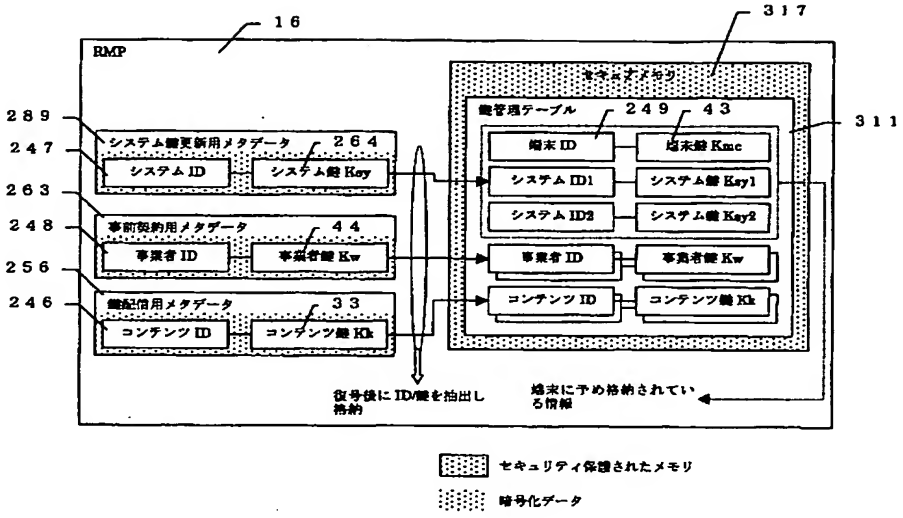
【図４４】



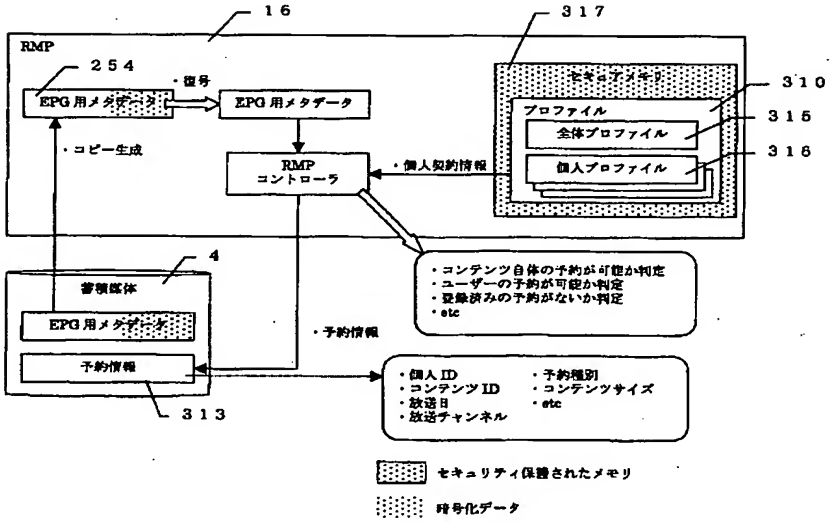
【図５１】

データ種別	暗号鍵種別	補足
コンテンツ	コンテンツ鍵（Kk）	コンテンツ毎に固有の鍵
メタデータリスト	無し	暗号化を行わない
事前契約用メタデータ	端末鍵（Knc）	端末毎に固有の鍵
EPG用メタデータ	システム鍵（Ksy1）	システム全体で共通の鍵
蓄積/再生用メタデータ	コンテンツ鍵（Kk）	コンテンツ毎に固有の鍵
鍵配信用メタデータ（無料）	システム鍵（Ksy1）	システム全体で共通の鍵
鍵配信用メタデータ（有料）	事業者鍵（Ky）	事業者毎に固有の鍵
システム鍵更新用メタデータ	システム鍵（Ksy2）	システム全体で共通の鍵（予備用）

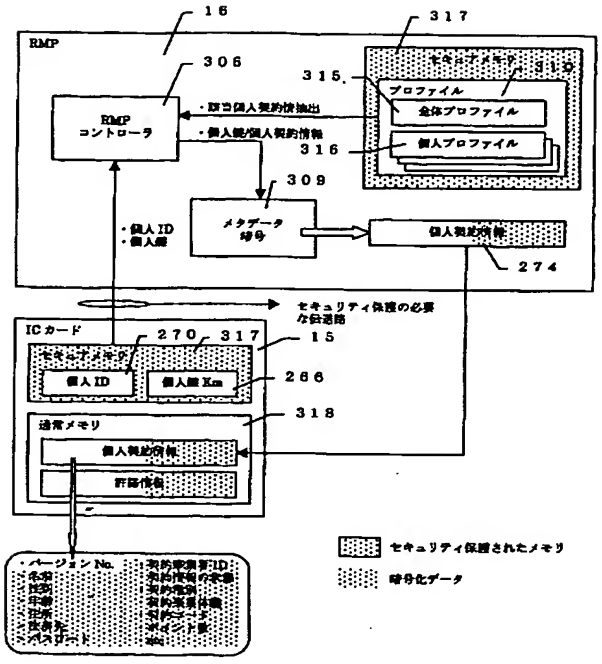
【図４５】


16
317
RMP
289
247
263
248
256
246
システム鍵更新用メタデータ
システム ID
システム鍵 Key
264
事前契約用メタデータ
事業者 ID
事業者鍵 Kw
44
鍵記信用メタデータ
コンテンツ ID
コンテンツ鍵 Kk
33
鍵管理テーブル
249
43
311
端末 ID
端末鍵 Kmc
システム ID1
システム鍵 Key1
システム ID2
システム鍵 Key2
事業者 ID
事業者鍵 Kw
コンテンツ ID
コンテンツ鍵 Kk
復号後に ID/鍵を抽出し格納
端末に予め格納されている情報
セキュリティ保護されたメモリ
暗号化データ

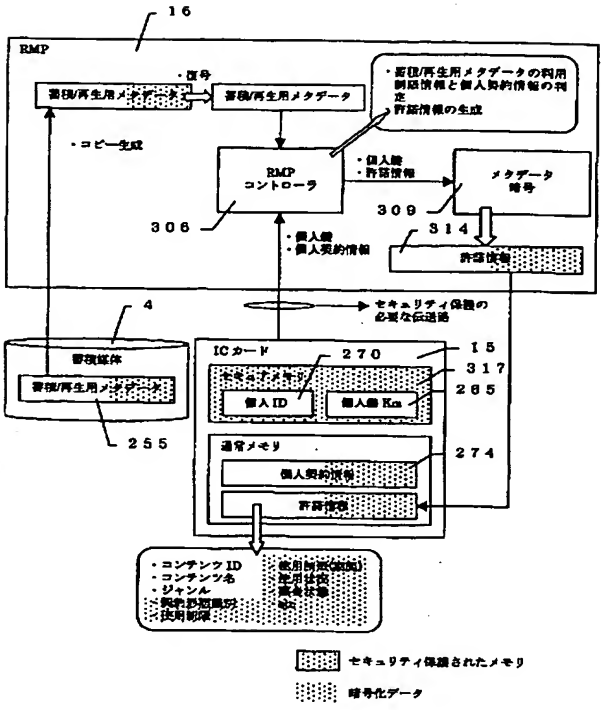
【図４７】


16
317
RMP
254
EPG 用メタデータ
・復号
EPG 用メタデータ
・コピー生成
RMP
コントローラ
・個人契約情報
セキュアメモリ
310
プロファイル
315
全体プロファイル
316
個人プロファイル
4
蓄積媒体
EPG 用メタデータ
予約情報
313
・予約情報
・コンテンツ自体の予約が可能か判定
・ユーザーの予約が可能か判定
・登録済みの予約がないか判定
・etc
・個人 ID
・コンテンツ ID
・放送日
・放送チャンネル
・予約種別
・コンテンツサイズ
・etc
セキュリティ保護されたメモリ
暗号化データ

【図４８】



【図４９】



【図５２】

RMP コントローラの主な機能

機能	内容
受信制御	・蓄積/再生用メタデータ、鍵配信用メタデータ、プロファイルより受信可能なコンテンツかを判断し、コンテンツの受信を制御する機能
蓄積制御	・RMP 内部で発生するコンテンツ、メタデータ等の蓄積媒体への蓄積動作を EPG 用メタデータ、蓄積/再生用メタデータ、メタデータリスト等により制御する機能
コピー制御	・視聴契約等のユーザーリクエスト等により発生するリムーバブルメディア等へのコピー要求を蓄積/再生用メタデータの情報により制御する機能
提示制御	・ユーザーの視聴要求に対し蓄積/再生用メタデータの情報、視聴契約により生成された許諾情報をもとにコンテンツの再生を制御する機能
視聴契約制御	・蓄積/再生用メタデータ、IC カード内の個人契約情報をもとにコンテンツの視聴に対する許諾情報を生成する機能
課金制御	・蓄積/再生用メタデータに格納されたポイント情報等と、IC カード内の個人契約情報をもと行われる課金処理を制御する機能
個人認証制御	・各メタデータ内にユーザーを制限する情報がある場合に、プロファイル、IC カード内の個人契約情報をもとに行われる認証処理を制御する機能
鍵管理	・受信端末内の鍵を管理する機能
プロファイル管理	・事前契約用メタデータから生成される各個人、端末のプロファイルを管理する機能
時刻管理	・受信端末における時刻情報を管理する機能
アプリケーション認証制御	・Plug in アプリケーション等に対する認証を制御する機能
外部機器認証制御	・受信端末に接続される外部機器に対する認証を制御する機能
通信回線制御	・視聴履歴、課金情報等の権利保護が必要な情報を通信回線を利用し送出側に送信する際に通信路の安全性に関する制御を行う機能

フロントページの続き

(51)Int.Cl.'	識別記号	FI		テーマコード(参考)
Ｈ０４Ｎ　5/76		Ｈ０４Ｎ	7/173	６４０Ａ
5/91		Ｈ０４Ｌ	9/00	６０１Ｂ
7/167		Ｈ０４Ｎ	7/167	Ｚ
7/173	６４０		5/91	Ｐ

(72)発明者　山崎　伊織
東京都千代田区神田駿河台四丁目６番地
株式会社日立製作所放送・通信システム推進事業部内

Ｆターム(参考)　5C052 AB02 CC01 DD04 DD06
5C053 FA20 FA28 GB05 JA21 LA11 LA15
5C064 BB01 BB02 BC04 BC17 BC22 BC23 BC25 BD08 BD09
5J104 EA10 EA17 NA02 PA05 PA11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/007235

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F17/60

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2004
Kokai Jitsuyo Shinan Koho 1971-2004 Jitsuyo Shinan Toroku Koho 1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JICST FILE(JOIS), WPI, INSPEC(DIALOG)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2002-279211 A (Oki Electric Industry Co., Ltd.), 27 September, 2002 (27.09.02), Figs. 1 to 2 (Family: none)	1-26
Y	JP 2002-169912 A (Hitachi, Ltd.), 14 June, 2002 (14.06.02), Full text; Figs. 1 to 13 (Family: none)	1-26
Y	JP 11-272762 A (Hitachi, Ltd.), 08 October, 1999 (08.10.99), Full text; Figs. 1 to 21 (Family: none)	1-26

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
08 July, 2004 (08.07.04)	27 July, 2004 (27.07.04)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/007235

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2001-83874 A (Sony Corp.), 30 March, 2001 (30.03.01), Full text & WO 1019017 A1 & JP 13-076425 A & JP 13-075871 A & JP 13-075923 A & JP 13-075930 A & JP 13-092880 A & JP 13-094554 A & EP 1128598 A & CN 1322422 A	1-26
A	JP 2000-148861 A (Sony Corp.), 30 May, 2000 (30.05.00), Full text; Figs. 1 to 15 & WO 029996 A1 & EP 1071031 A1 & CN 1293786 T & US 2001/0047317 A1 & US 2001/0047318 A1 & US 2003/0004841 A1	1-26
A	JP 2002-217894 A (Hitachi, Ltd.), 02 August, 2002 (02.08.02), Full text; Figs. 1 to 52 (Family: none)	1-26